University of Tampere
School of Management

FRAUD PREVENTION AND DETECTION METHODS IN RUSSIAN SMALL-SCALE ENTERPRISES: PERCEPTIONS OF MANAGERS AND ACCOUNTANTS REGARDING THEIR EFFECTIVENESS

Accounting and finance
Master's Thesis
August 2013
Supervisor: Professor Lili Kihn
Milyutina Ekaterina

ABSTRACT

University of Tampere:	School of Management
Author:	MILYUTINA EKATERINA
Title:	Fraud Prevention and Detection Methods in Russian Small-Scale Enterprises: Perceptions of Managers and Accountants Regarding Their Effectiveness
Master's Thesis:	58 pages and 4 appendices
Discipline:	Accounting and Finance
Date:	August 2013
Key words:	Fraud, Prevention, Detection, Effectiveness, Usage, Small Businesses

---

Previous studies of fraud prevention and detection in Russian business environment have primarily targeted large-scale organizations. Meanwhile, small businesses are particularly vulnerable to deception due to lack of resources that large companies have to elaborate internal control.

The purpose of this research is to identify effective methods to fight asset misappropriation, in particular billing, payroll and expense reimbursement schemes, in Russian small businesses. This is achieved by answering the following research questions: What measures do fraud experts recommend to prevent and detect billing, payroll and expense reimbursement schemes? What measures do Russian small businesses have in place to prevent and detect billing, payroll and expense reimbursement schemes? How do managers and accountants estimate effectiveness of the measures in preventing and detecting billing, payroll and expense reimbursement schemes?

The data used in this study was gathered carrying out an analysis of the content of recent fraud literature and conducting an e-mail survey. A total of 14 small business managers and accountants responded to the questionnaire (response rate 100%). Because of non-random selection of the survey participants, there might be a difference between the results from the current study and the results from the entire population

It was found that managers and accountants in small businesses believe the most effective fraud detection procedures are comparing purchase order with invoice and with shipping documents and confirming data with vendors/customers. They rate having restricted access to business records in organization as the most effective fraud prevention measure, while fraud detection training is viewed as the least effective measure.

TABLE OF CONTENT

1. INTRODUCTION.....4

1.1. Background of the topic……...4

1.2. Purpose of the study……6

1.3. Contribution of the study……8

2. THEORETICAL BACKGROUND……..11

2.1. Fraud theory……....11

2.2. Asset misappropriation…….....14

2.2.1. Billing schemes…….....16

2.2.2. Payroll schemes…….....19

2.2.3. Expense reimbursement schemes…….....23

2.3. Asset misappropriation prevention and detection in Russian small business environment……..….27

2.4. Theory summary…….....33

3. METHODOLOGY……..37

3.1. Research design……..37

3.1.1. Content (conceptual) analysis.....37

3.1.2. Survey design……38

3.2. Sample……43

3.3. Reliability and validity……46

4. RESULTS OF THE SURVEY……..….47

4.1. Use and effectiveness of fraud prevention and detection methods……..….47

4.2. Discussion and recommendations.....52

5. CONCLUSION.....57

REFERENCES.....59

APPENDICES.....64

1. INTRODUCTION

1.1. Background of the topic

The research is motivated by the findings of several surveys separately conducted by PricewaterhouseCoopers (PwC) and Association of Certified Fraud Examiners (ACFE). The 2011 study[1] by PwC presents a picture on economic crime situation in Russia, where asset misappropriation[2] is considered to be the most common type of violation. Although the research reveals a decline in the reported fraud incidents over the past few years, most respondents express concern of being economic crime victims. The survey data on the actual cases of violations and methods of their detection was obtained from Russian leading organizations of diverse sizes – those employing less than 1000 persons, 1001 to 5000 persons, and over 5000 persons.

At the same time, ACFE conducted a study[3] of business security risks in Russian companies. The research reports on fraud[4] as the most significant threat and source of losses in the entities, and presents rating of measures carried out by companies to combat violation. The survey data was received from employees of the most advanced entities in terms of business security technologies. The majority of the respondents worked in companies with more than 500 staff.

The 2012 study[5] by ACFE examines occupational fraud[6] and methods to secure business from losses caused by illegal acts of staff members. The research has summarized information on offences occurred in different countries, which clearly indicates small businesses – organizations with fewer than 100 employees – have consistently experienced the greater percentage of the fraud cases than large companies.

---

[1] http://www.pwc.ru/en_RU/ru/forensic-services/assets/Economic-survey-2011-Russia-en.pdf
[2] Theft or misuse of company assets.
[3] http://acfe-rus.org/
[4] Intentional crime against company property, including corruption.
[5] http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf
[6] The use of one's occupation for personal financial gain through the deliberate misuse or misapplication of company resources or assets.

Despite the surveys address information to fraud and its detection, none of them sufficiently investigates methods that would help small entities to fight against violation. Small businesses are particularly vulnerable to deception due to lack of resources that large companies have to elaborate internal control[7] (Johnson, Rudesill, 2001; Wells, 2003; ACFE, 2012: 5). In addition, because of fewer funds, the losses from offences experienced by small entities tend to have a greater impact than they would in larger organizations (ACFE, 2012: 5). Nevertheless, the professional literature on fraud prevention and detection commonly targets a general business audience and rarely discloses such issue in the context of small enterprises. In particular, Bierstaker, Brody and Pacini (2006) present a list of anti-fraud methods that small entities may be unable to employ due to their high cost. Likewise, Vanasco (1998) in his extensive research provides a platform for fraud detection and deterrence procedures that could be carried out by internal auditors and top management, meaning larger organizations.

Johnson and Rudesill (2001), although investigate topic in question in small businesses, come up with generalized defense practices and audit procedures aimed to prevent and detect a wide range of deceptions. Meanwhile, some violations may require special treatment. Therefore, a focus on individual fraud schemes can bring a certain concretization in the list of fraud prevention and detection methods. Additionally, looking into specific offences that pose a serious threat to the business can help define the areas that require immediate management's attention in order to avoid losses. Since no paper examines in detail protection of small entities from fraud[8], a research is needed to study measures, owners and managers of small enterprises can apply to prevent and detect the most likely violations. Furthermore, restricted amount of organization's resources indicate the demand of using the "best" techniques to combat fraud, avoiding investments in costly control mechanisms.

Based on the corporate fraud, forensic accounting and fraud auditing literature, this study concentrates on methods intended to secure small businesses from asset

[7] According to the framework from the Committee of Sponsoring Organizations of the Treadway Commission (COSO 1992), internal control is a process designed to provide reasonable assurance over the achievement of objectives concerning effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

[8] In this study, the term "fraud" refers to occupational/internal fraud, often called white-collar crime.

misappropriation, most prevalent deception within such entities (ACFE, 2012: 27). The topic is examined in the context of Russian business environment, as economic crime is and will remain a very serious risk for Russian organizations (PwC, 2011; ACFE, 2011). The research investigates availability of anti-fraud measures in Russian small enterprises[9] and perception of insiders about effectiveness[10] of the measures in preventing and detecting violation.

1.2. Purpose of the study

The main purpose of the study is to identify effective methods to fight white-collar crime in Russian small businesses. It can be divided into three parts. The first sub-purpose is to explore the common ways asset misappropriation schemes are prevented and detected. The second sub-purpose is to examine the use of anti-fraud methods in Russian small organizations. The third sub-purpose is to investigate opinions of managers and accountants regarding effectiveness of the methods in preventing and detecting illegal activities.

The first part of this paper deals with policies and procedures aimed to protect companies from asset misappropriation. The section is built on the fraud theory, which defines asset misappropriation schemes and their characteristics alongside with the red flags[11] associated with the deceptions (Singleton, Singleton, 2010: 94, 95). Anti-fraud policies and procedures are identified with the help of the red flag approach, which is based on searching for anomalies in business (Carmichael, Graham, Whittington, 2007: 140). The paper comes up with a list of methods designed to detect the warning signals and reduce the risk of fraud occurrence.

[9] According to Russian Federal Law № 209-FZ, 24 July 2007, small business comprises sole proprietorship, micro- and small-sized companies that meet criteria based on ownership structure, revenue volume and number of employees. In the current paper, "small enterprise" is referred to companies and sole proprietorship with fewer than 100 staff.
[10] The capability of producing a desired result.
[11] Traces of the criminal and crime left at the scene of the crime, or in the fraudster's life.

The emphasis of the study is put on asset misappropriation, in particular cash misappropriation, due to its significant prevalence in the entities world-wide (ACFE, 2012: 12). The following cash misappropriation schemes are examined: billing, payroll and expense reimbursement. The choice was made on the ground of several findings. All the offences belong to the fraudulent disbursement, which remains the largest defalcation scheme in accounting. Besides, within this category, billing, payroll and expense reimbursement are the dominant frauds perpetrated against small businesses (Gramling, Johnstone, Rittenberg, 2011: 453, 454; ACFE, 2012: 12, 27). The research excludes investigation of check tampering, as checks are not widely used in Russia, and their share in the total volume and value of payments does not exceed 1% (CPSS, 2011: 303).

The second part of this paper focuses on the employment of anti-fraud methods in Russian small enterprises and effectiveness of the methods in preventing and detecting white-collar crime. Based on the literature review, accountants and managers are asked to indicate anti-fraud policies and procedures used in their small organizations. In addition, respondents are asked to rate effectiveness of policies and procedures in combating illegal activities. The section results in a list of the most effective and ineffective fraud prevention and detection methods.

Although studies on fraud prevention and detection are commonly based on the surveys of accounting practitioners, researches of this type may involve some risk of respondent bias. Accountants are likely to understand basic forensic accounting/audit terminology and are more likely than other specialists in small organization to answer the questions on combating fraud. However, at the same time, there is a possibility that, due to professional activity, respondents are competent in fraud detection rather than prevention, and therefore may rate effectiveness of defense practices superficially. Meanwhile, it is the responsibility of an organization’s management to design and review policies and procedures that will deter and/or detect illegal activities (Johnson, Rudesill, 2001). Hereby, questioning accountants alone cannot provide reliable information on what methods are effective in fighting white-collar crime. Therefore, the

participants of the current research include both accountants and managers from different organizations.

The research question of this study is: What measures are effective in preventing and detecting billing, payroll and expense reimbursement schemes in Russian small businesses?

The research sub-question 1 is: What measures do fraud experts recommend to prevent and detect billing, payroll and expense reimbursement schemes?

The research sub-question 2 is: What measures do Russian small businesses have in place to prevent and detect billing, payroll and expense reimbursement schemes?

The research sub-question 3 is: How do managers and accountants estimate effectiveness of the measures in preventing and detecting billing, payroll and expense reimbursement schemes?

1.3. Contribution of the study

Fraud can affect any organization, and its impact on reputation and financial health can be enormous. One of the most effective ways to deal with the growing threat of fraud is to understand the fraud concept, recognize red flags and be proactive about spotting business anomalies. In fact, many studies describe recognition of white-collar crime from the perspective of auditors and fraud examiners. However, small businesses often can not afford to hire internal auditor or conduct regular external audit, due to lack of funds. Therefore, owners and managers of small organizations hunt for information on common and inexpensive fraud prevention and detection methods. Meanwhile, a large number of fraud incidents shows a strong need for the research that proposes the “best” measures to fight illegal activities.

Covering the nature of fraud and its types, this study provides a list of fraud prevention and detection methods and their effectiveness ratings. The paper contributes to the existing research in several respects. First, the study examines policies and procedures intended to prevent and detect cash misappropriation schemes in Russian small businesses. Fraud itself has continued to prosper, while information on effective methods to fight it has largely dissipated. The current literature has gathered a big variety of anti-fraud measures employed in the entities worldwide. However, there is not much survey evidence about their effectiveness. Thus, this subject deserves more research attention.

Additionally, the prior studies targeted mostly the largest companies, while the opportunity for fraud is greater in smaller organizations. In particular, Russian body of research (e.g., ACFE, 2011; PwC, 2009; 2011) does not provide information on the ways to combat white-collar crime in small entities. Meanwhile, according to statistical data[12, 13] as of the end of 2010, small businesses make up a significant contribution to Russian economy and comprise a vast majority of the commercial organizations in the country. Thus, there is a room (and need) for further investigation into fraud prevention and detection, with a focus on small enterprises.

Second, the research gathers information on simple checks that can be used by non-fraud experts to prevent and detect violations. The study examines various audit procedures and addresses them to the fraud indicators, giving a tip about the anomaly to search for when applying a certain method. The research helps owners and managers of small businesses understand how certain types of fraud occur, what symptoms the schemes leave behind and how to prevent and recognize potential illegal activities. At the same time, the paper provides prescriptive information on what anti-fraud methods work the "best". Business owners and managers may wish to consider investing in the methods in order to prevent common frauds in their organizations.

Third, there is a lack of knowledge on the effectiveness of fraud prevention and detection techniques from the managers' opinion. The earlier studies, such as Johnson

[12] http://www.rcsme.ru/eng/common/totals.asp
[13] http://www.gks.ru/bgd/regl/b11_12/IssWWW.exe/Stg/d01/13-01.htm

and Rudesill (2001), Brody and Pacini (2006), paid attention to the accounting practitioners' estimation, despite the fact that establishing, maintaining and enforcing anti-fraud policies and procedures are the responsibility of the organization's management (ISA 240[14]; SAS 99[15]). Moreover, Johnson and Rudesill (2001) in their work pointed out at the effectiveness of owners and managers in detecting illegal activities. Thereat, the present paper examines perception of both accounting and management practitioners.

Fourth, the research overcomes some methodological limitations that belong to the prior studies. For example, Johnson and Rudesill (2001), while investigating occupational fraud in small businesses, did not define fraud in the survey instrument, making it possible that respondents might have included external fraudulent activities in formulating their answers. Brody and Pacini (2006), while gathering data on the use of fraud prevention and detection techniques, did not give explanation of fraud procedures and software in the questionnaire, thus, introducing a risk that study participants might have misunderstood specific forensic accounting/audit wordings. In this respect, the current research employs the survey instrument that provides basic fraud terminology, as well as interpretation of defense practices and audit procedures.

Additionally, ACFE (2012), although included small businesses into the study, only focused briefly on the aspect of fraud prevention and detection and did not provide any guideline on the application of anti-fraud methods for organizations. On the contrary, this paper gives recommendations to small business owners and managers on the use of some cost-effective[16] anti-fraud techniques.

[14] International Standard on Auditing (ISA) 240, December 2009, "The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements."
[15] Statement on Auditing Standards (SAS) 99, October 2002, "Consideration of Fraud in a Financial Statement Audit."
[16] Providing adequate results in relation to incurred costs.

2. THEORETICAL BACKGROUND

The initial step in fighting against fraud is to understand its origin and characteristics. Therefore, at the beginning of this chapter a fraud theory is presented, defining the principles of fraud and essentials of fraud prevention and detection. The second section discloses characteristics of common cash misappropriation schemes along with the red flags associated with illegal activities and anti-fraud measures. The third section presents policies and procedures aimed to prevent and detect fraud in Russian small business environment. The fourth section summarizes findings derived from the theoretical chapter.

2.1. Fraud theory

The Institute of Internal Auditors (IIA) in the Standard 1210.A2 presents fraud as a range of irregularities and illegal acts characterized by intentional deceit or misrepresentation. Fraud is perpetrated by a person outside and inside the organization for his or her benefit, for the benefit of the organization or another person. From the above definition, white-collar crime is seen as a dishonest act committed by insiders for their own purposes or enrichment, rather than for the enrichment of the organization on a whole, in spite of supposed corporate loyalty. The reasons why occupational fraud is common among trusted individuals can be found in behavioral theories of financial crime that explain individualistic aspects of natural phenomena (see Gottschalk, 2010: 211-212). One of them, fraud theory, defines in detail conditions of the fraud risk.

In the 1950s Donald Cressey developed the fraud triangle model, explaining the factors that cause individual to commit occupational fraud (see Figure 1). Cressey concluded that there are three requirements for fraud to occur: incentive or pressure (e.g., a need for money), opportunity (e.g., weaknesses in internal controls[17]) and personal characteristics or rationalization (e.g., willingness to commit fraud). The incentive to commit fraud is associated with personal pressures and/or corporate pressures on the

[17] A set of policies and procedures to prevent wrong actions from occurring (COSO, 1992).

individual. Opportunity appears when there is an easy access to company's assets or when an individual manages a control procedure that assists in accomplishing a deceit. One's job position, responsibilities and authorization also contribute to the opportunity to commit fraud. Personal characteristics imply an attitude, character, or set of ethical values that enables an individual to justify a dishonest act (Vona, 2008: 7-8). To sum up, occupational fraud is most prevalent in organizations that have no controls, no ethical standards and no profits. Likewise, the more these conditions exist, the higher the risk of fraud.

Figure 1. The fraud triangle (Wells, 2001)

The variety of fraud schemes is connected to the opportunity dimension of the triangle. Each fraud scheme occurs differently in each organization and industry, but its fundamental mechanics stays the same for all enterprises. Every single fraud scheme has a unique characteristics and concealment strategy that enables an individual to hide the fraudulent transaction. However, the way to implement the strategy can vary on one's position and company's internal controls. Each concealment strategy has related red flags that indicate a potential for a fraud scheme (Vona, 2008: 9-10, 13-14). They include accounting anomalies (e.g., incorrect ledger balances), analytical irregularities (e.g., inventory shortages), internal control weakness (e.g., a lack of proper authorization), changes in person's behavior or lifestyle, tips and complaints that something is wrong (Singleton, Singleton, 2010: 95-96; Carmichael, Graham, Whittington, 2007: 129-130).

The presence of red flags does not necessarily mean that fraud takes place, and can be provoked by non-fraud factors (Krambia-Kardis, 2002). For instance, unusual increase

in accounts receivable may be the result of deception, or may appear due to financial difficulties of major customers (Burke, Cooper, Tomlinson, 2010: 182). Therefore, the process of fraud detection centers on looking for anomalies in business and investigating whether signals observed represent actual violation or are the result of other events (Carmichael, Graham, Whittington, 2007: 140).

To have a high probability of fraud detection, owners and managers need to understand as many red flags as possible. General red flags, such as employee's change in lifestyle or behavior, tips and complaints that something is wrong, although indicate a fraud, are not necessarily connected to a specific violation. Therefore, an identification of those red flags associated with particular fraud schemes is even more important. A thorough understanding and analysis of such warning signals assist in developing potentially effective detection methods for certain types of violations (Singleton, Singleton, 2010: 111-112, 155).

Meanwhile, preventing fraud seems to be more desirable for organizations than detecting it. According to Treadway Commission findings, the most effective way to protect business from white-collar crime is to install a strong set of internal controls. The model developed by the group has come to be known as the COSO Model of Internal Controls. It focuses on five key areas:

1) control environment – a component that sets a fundamental discipline and structure of the organization's internal control system;
2) risk assessment – a process that involves identification, analysis and assessment of risks in the achievement of entity's objectives;
3) control activities – practices, policies and procedures that help ensure management directives are carried out;
4) information and communication – systems and reports that enable individuals to carry out their responsibilities;
5) monitoring – an external overview of internal controls.

Controls restrict the opportunity to commit fraud and warn potential fraudsters that management is actively monitoring the business that in turn deters illegal activities (Carmichael, Graham, Whittington, 2007: 128). However, unlike big enterprises, small entities may not need such internal control structure due to its costs and operational complexity. Nevertheless, owners and managers of small organizations still need to develop anti-fraud policies and procedures to prevent wrong actions from occurring.

The following section looks into billing, payroll and expense reimbursement schemes. Besides description of fraud categories and particular manipulations, the part presents the red flags associated with the schemes and ways to combat illegal activities. The research moves away from the general (environmental, cultural, and corporate) anti-fraud measures and concentrates on specific policies and procedures. The section lists defense practices that serve to minimize the risk of fraud in organizations (Vona, 2008: 225), and audit procedures that assist in searching for the fraud indicators sufficient to warrant recommending an investigation.

2.2. Asset misappropriation

Asset misappropriation involves converting to personal use company's assets (Johnson, Rudesill, 2001). The fraud is conducted by employees, against the organization, for the benefit of the perpetrator (Singleton, Singleton, 2010: 56, 62). While such detriment may seem insignificant on the daily basis, it can cause serious long-term damages over a period (Lasko, 2009). In 1996 ACFE in the Report to the Nation on Occupational Fraud and Abuse[18] presented the asset misappropriation chart, which is now known as the "fraud tree" (see Figure 2).

Assets that employees misappropriate can be divided into two groups: cash, inventory and all other assets. Most illegal schemes involve cash account, as cash is fungible and easy to transport (Wells, 2001). Such schemes are not limited to the theft of currency on

[18] http://www.acfe.com/documents/Report_to_the_Nation.pdf

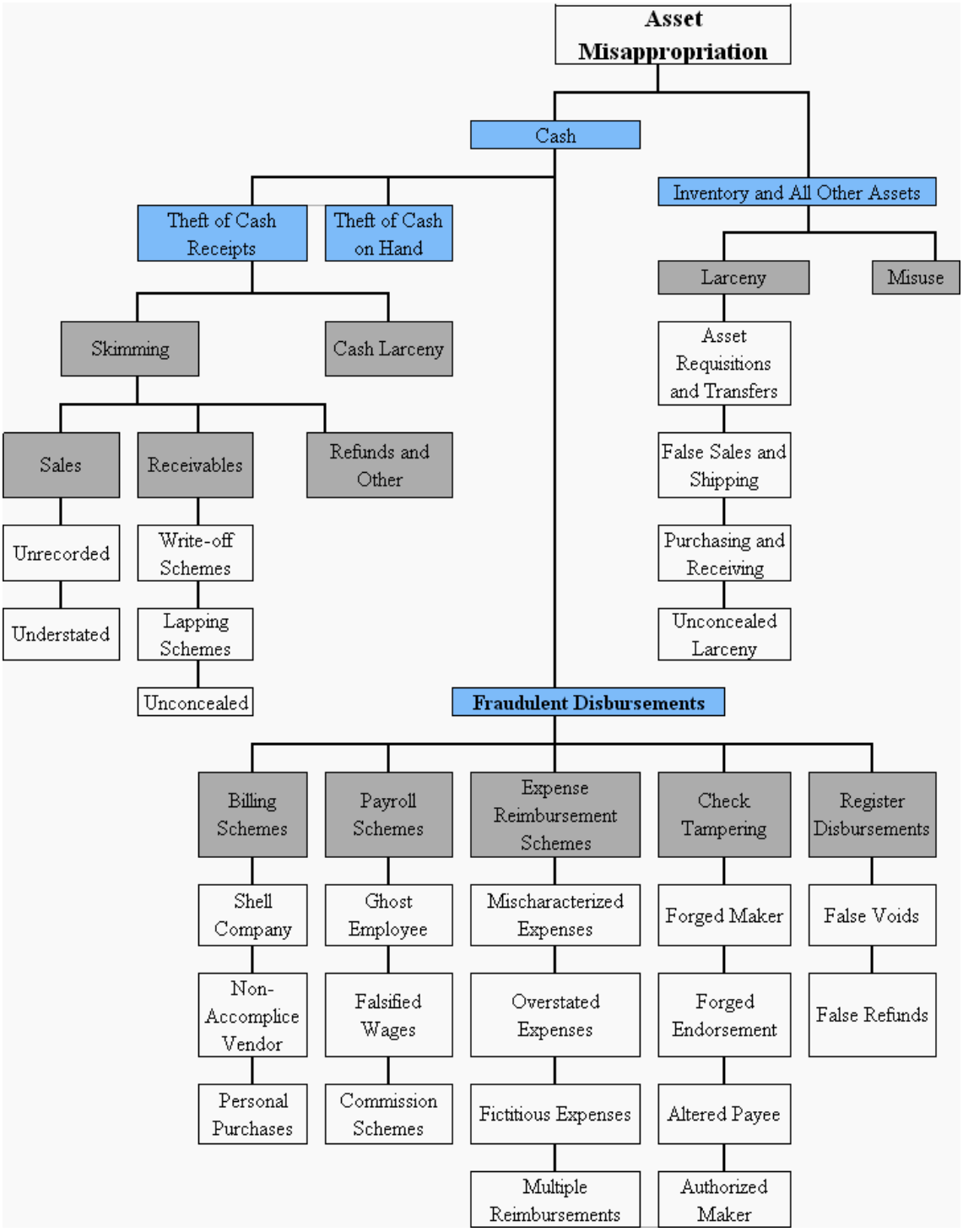

Figure 2. The fraud tree (ACFE, 2012)

hand, and imply complicated manipulations with checks and other financial instruments. Cash frauds can be divided into schemes related to cash receipts, cash on hand and cash disbursements (ACFE, 2012: 7).

Fraudulent disbursement is considered to be the most expensive cash fraud scheme, which implies disbursement of organization's funds caused by employee through some trick or device (Wells, 2003; 2004). The key feature of this crime lies in the former, an employee takes cash from the employer as if it is a legitimate transaction (Singleton, Singleton, 2010: 86). Fraudulent disbursements can be categorized into billing schemes, payroll schemes, expense reimbursement schemes, check tampering and register disbursements (ACFE, 2012: 7).

2.2.1. Billing schemes

Billing schemes imply a false invoice (i.e., invoice for fictitious goods or services, inflated invoice, or invoice for personal purchases) submitted by employee the company unknowingly pays to the benefit of the thief (Wells, 2003; 2004; ACFE, 2012). Such fraud can be perpetrated through the use of a shell company scheme, non-accomplice vendor scheme or personal purchases scheme (ACFE, 2012: 7).

A shell company is an entity without active business purpose, typically created for conducting an illegal activity. The company has no physical address, no employees, and does not have any goods or services to offer. However, it is legally incorporated, and files tax returns (Vona, 2008: 83). In *a shell company scheme* an employee sets up a fictitious company causing his employer to pay for its non-existed goods or services (Goldmann, Kaufman, 2009: 27). The fraud is accomplished by submitting a false invoice, approving the invoice, issuing payment to the shell vendor, and intercepting the payment by the fraudster or an accomplice (Singleton, Singleton, 2010: 87). The scheme goes beyond the invoices for fictitious goods and services, and also includes inflated invoices. In this case, employee orders merchandise from the legitimate vendor, and then by setting up the pseudo vendor sells the goods to his employer at the inflated price (Goldmann, Kaufman, 2009: 29).

In order to prevent a shell company scheme from occurring, the duties in the purchasing process should be separated, i.e., different people are responsible for requisitioning

goods or services, purchasing, approving purchases, issuing and recording related payments, and receiving the merchandise (Singleton, Singleton, 2010: 123; Wells, 2011: 204). Such measure deters employee from having too much control over the process and thus, decreases an opportunity to commit the offence (Coenen, 2008: 154; COSO, 2006: 5).

As the scheme deals with invoicing from fictitious vendors, it is important to maintain and regularly update an approved vendor list[19]. Before adding a new vendor to the list, entity's legitimacy must be verified by someone independent of the purchasing function (Kranacher, Riley, Wells, 2010: 329). Verification can be done, for instance, by obtaining company's corporate records and other relevant documents (Wells, 2002). Apparently, an invoice from the entity that is not on the approved vendor list might indicate the fraud. A simple comparison made between invoices and the accounts payable list of vendors can reveal the red flag (Goldmann, Kaufman, 2009: 47, 82).

Sometimes perpetrators may use their own home address, initials or bank account when setting up a shell entity. Therefore, any matches between employee data and vendor data might indicate an existence of phantom company. By comparing relevant data, a victim entity can detect the fraud signal (Vona, 2008: 86-87; Coenen, 2008: 81).

In a shell company scheme a dishonest employee usually bills his employer for services rather than goods. Purchases of fictitious goods cause inventory shortages as the items appear only in the company's inventory system. By conducting a stock-taking, i.e., comparing physical inventory to purchases, an employer can easily reveal non-existed merchandise. Fictitious services are more difficult to trace due to their intangibility. However, such purchases cause an increase in the service-related expenses that can serve as an indicator of the scheme. Other red flags associated with the fraudulent purchases include unusual or unexpected growth in cost of goods sold and average unit price of items acquired. This kind of anomaly can be detected through trend analysis,

[19] A list of vendors considered as acceptable to buy from. Each approved vendor has a file, containing key information about company (Goldmann, Kaufman, 2009: 47, 52). In this study, the term approved vendor list, also referred to as accounts payable list of vendors, includes both list of vendors and relevant files.

i.e., comparison of the same financial data on a year-to-year basis (Kranacher, Riley, Wells, 2010: 328-330; Singleton, Singleton, 2010: 105).

There are certain signals that indicate a potential for shell company invoices. They include a lack of information on the invoice and sequential invoice numbers from a vendor. Detection of the fraud indicators can be conducted through the review of invoices sorted according to the vendor and document number. Additional attention should be paid to the quantities and types of goods and services the company purchases. Odd items on the invoices and high level of purchases might signal a fraudulent activity. By monitoring the nature and quantities of goods and services acquired, an employer can detect the red flags (Kranacher, Riley, Wells, 2010: 329-330).

In *a non-accomplice vendor scheme* an employee intentionally mishandles payments intended for a legitimate vendor. For instance, the perpetrator double-pays an invoice on purpose, then requests to return one of the payments and intercepts it. Similarly, the fraudster intentionally pays the wrong vendor or pays the proper one, but purposely overpays him. Also an employee might overbill a victim company by submitting a fake invoice in the name of a legitimate vendor with further interception of the payment (Kranacher, Riley, Wells, 2010: 331). Another version of the scheme is to order merchandise not needed, then return the merchandise to the vendor and pocket the refund (Singleton, Singleton, 2010: 87).

When submitting a fake bill in the name of a legitimate company, the perpetrator might change the vendor's data, in order to collect the payment. By reviewing the accounts payable list of vendors, an employer can reveal data mismatch. In addition, a counterfeit invoice might have a significantly out of sequence number, which is easily detected when sorting invoice numbers from a particular vendor. Instead of producing fake bills, a dishonest employee may rerun invoices from the legitimate vendors and intercept the payment resulted from the second run. In this case, duplicate invoice numbers can be detected through the review of paid invoice data. To prevent the fraud, a victim entity can use the same methods as in a shell company scheme – segregation of duties in the

purchasing process and maintenance of an approved vendor list (Kranacher, Riley, Wells, 2010: 332).

In *a personal purchases scheme* an employee causes his employer to pay for personal items (Singleton, Singleton, 2010: 87). Usually the fraud is committed through submission of false invoices. The perpetrator buys an item, and then presents the bill to the employer as if the acquisition has been made on behalf of the company. Another way to make personal purchases with the employer's money involves the misuse of entity credit cards (Kranacher, Riley, Wells, 2010: 333, 336).

To accomplish the scheme, fraudsters may change the delivery address for supplies, so that the merchandise would arrive directly to their home or business. Therefore, shipments to locations other than company are a potential fraud signal. By reviewing invoices, an employer can detect address discrepancy (Kranacher, Riley, Wells, 2010: 333, 339). Other red flags associated with the deception involve purchases of unusual items that have no business purpose and increase in expenditures. Examination of invoices (Vona, 2008: 101) or an independent review of the credit card statement can reveal the acquisition of goods in question, while trend analysis of vendor payments can uncover an unexplained tendency (Kranacher, Riley, Wells, 2010: 337; Wells, 2011: 200).

In order to prevent the fraud, the duties in the purchasing process should be properly segregated, so that no one could approve the acquisition of personal items (Kranacher, Riley, Wells, 2010: 333). Establishing maximum purchasing limits for each employee (Wells, 2002) may not deter the scheme from occurring, but can restrict damages from deception (Kranacher, Riley, Wells, 2010: 337). Table 1 summarizes the red flags associated with the billing schemes and methods of fraud prevention and detection.

2.2.2. Payroll schemes

Payroll schemes involve false claims for compensation submitted by employee the

Table 1. Billing schemes

Red flags	Prevention methods	Detection methods
▪ Matches between an employee's home address/initials/bank account and vendor's address/name/bank account ▪ Inventory shortages ▪ Unusual or unexplained increase in cost of goods sold/service-related expenses/average unit price of items acquired/vendor payments ▪ Sequential invoice numbers from a vendor ▪ Out of sequence invoice numbers from a vendor ▪ Duplicate invoice numbers from a vendor ▪ Lack of detail on invoice ▪ Unusually high level of purchases ▪ Delivery address for purchases is different from the business address ▪ Purchases of unusual items ▪ Invoice from the vendor that is not on the approved vendor list ▪ Mismatch in vendor's data	▪ Segregation of duties between requisitioning goods or services, purchasing, approving purchases, issuing and recording related payments, and receiving the merchandise ▪ Maintaining and regularly updating an approved vendor list ▪ Independent verification of entity's legitimacy before adding a new vendor to the approved vendor list ▪ Segregation of duties between adding a new vendor to the approved vendor list and approving purchases ▪ Establishing maximum purchasing limits for each employee	▪ Comparing vendor data with employee data ▪ Stock-taking ▪ Trend analysis ▪ Sorting invoices by vendor and invoice number ▪ Examination of invoices/review of the credit card statement ▪ Monitoring the nature and quantities of goods and services acquired ▪ Comparing invoices with approved vendor list

company pays. The deception can be committed through ghost employee scheme, commission scheme, or falsified wages scheme (ACFE, 2012: 7, 12). Unlike billing frauds, payroll schemes imply disbursements to employees rather than to external parties (Wells, 2011: 208).

Ghost employees are individuals presented on the payroll[20], who are not providing services, but who are receiving payment (Vona, 2008: 145). The ghost can be a real person or a fictitious one invented by the perpetrator. The most common way to commit

[20] A form that contains a list of employees and amount of compensation that is due each pay period.

a ghost employee scheme implies adding a ghost employee to the payroll, approving a time sheet[21] or salary, issuing paycheck to the ghost, and intercepting the paycheck by the fraudster or an accomplice (Singleton, Singleton, 2010: 88).

When creating a ghost employee, the fraudster might fail to provide certain details (e.g., social security number, physical address, phone number, etc.), the omission of which is a red flag. Also a purely fictitious employee may have the same home address or bank account as the perpetrator. The fact that two employees are receiving payments at the same destination, have the same social security number or contact data may indicate the existence of a ghost on the payroll (Kranacher, Riley, Wells, 2010: 361, 362). Paychecks for employees who do not have any deductions or taxes withheld, who never take a vacation or sick leave, and who have a date of paycheck after termination, also represent a fraud signal (Singleton, Singleton, 2010: 107). Examination of payroll files[22] by someone independent of the payroll function can detect all these warning signs (Kranacher, Riley, Wells, 2010: 362; Singleton, Singleton, 2010: 152).

Reconciliation of employees in the payroll database with employees in the human resources database can reveal ghosts - persons on the payroll who have no personnel file[23] (Kranacher, Riley, Wells, 2010: 362; Singleton, Singleton, 2010: 168). Unexplained or unusual increase in wages expense - a signal of fraudulent activity - is easily detected through trend analysis (Singleton, Singleton, 2010: 107).

One of the basic methods to prevent a ghost employee scheme involves segregation of duties. In particular, hiring function should be separated from other payroll duties, so that no one could add a ghost employee to the payroll. By conducting background and reference checks before hiring (e.g., verifying educational credentials of a candidate), an employer can eliminate most ghost employee schemes (Kranacher, Riley, Wells, 2010: 362).

[21] A sheet that records actual number of hours worked by an employee during a pay period (Wells, 2011: 215).
[22] The employee payroll file is the repository for all records related to an employee's paycheck.
[23] A file that contains all records related to an employee's employment.

Commission is a form of compensation taken as a percentage from sales generated by employee. There are two factors that influence the amount of the commissioned wages: the size of generated sales and the percentage of those sales paid to an employee (Kranacher, Riley, Wells, 2010: 365). To falsely increase the pay, and thus to perpetrate *a commission scheme*, a fraudster may use one of the following methods: generate bogus sales, overstate sales, or increase the commission rate (Singleton, Singleton, 2010: 88).

One of the ways to detect a commission scheme is to examine correlation between sales figures and commission expenses. If commission expenses increase as a percentage of total sales, that might be a red flag. When a perpetrator commits the scheme, the commissions he/she earned will tend to be higher compared to the coworkers. By running a comparative analysis of commission earned by each employee, a victim entity can reveal the fraud signal (Kranacher, Riley, Wells, 2010: 367). At the same time, trend analysis can assist in monitoring changes in commission expenses, increase of which might be a warning sign (Singleton, Singleton, 2010: 108).

When the perpetrator creates fictitious sales to manipulate the pay, the sales usually stay uncollected. By tracking down uncollected sales generated by each employee, an employer can define if one has extremely bigger amount of these sales compared to the coworkers. In addition, getting independent data confirmation from customers can uncover both fictitious and overstated sales (Kranacher, Riley, Wells, 2010: 367).

To change the commission rate, and thus to commit the scheme, the fraudster may need to alter payroll or personnel files. Therefore, the access to such records should be off-limits to employees who receive commissioned wages (ACFE, 2007: 1.564).

Falsified wages scheme implies usage of the falsified hours worked and salary scheme (Singleton, Singleton, 2010: 88). For hourly employees, two main factors affect the size of a paycheck: the number of hours worked and the rate of pay. To fraudulently increase the size of wages, a perpetrator falsifies one of these elements. For salaried employees,

the most common way to generate fraudulent wages is to increase the rate of pay (Kranacher, Riley, Wells, 2010: 362).

When the rate of pay is falsely altered, mismatch between payroll and personnel data might appear. Such kind of anomaly can be detected by verifying the rates of pay in a pay period or for an employee over pay periods, i.e., comparing rates paid with the approved ones stored in the personnel files. Unexpected increase in wages expense is another red flag associated with the scheme, which can be uncovered by performing trend analysis. Verification of hours worked, i.e., comparison between hours paid and hours presented on employee time sheets, can show whether false amount is paid to an individual (Singleton, Singleton, 2010: 108, 153).

Other tests that can highlight falsified hours and salary schemes include running comparison reports of overtime generated by employee and making comparison between payroll expenses and budget projections. Such controls can reveal variations from budgeted expenses and detect whether a particular individual has significantly bigger amount of overtime paid compared to the coworkers (Kranacher, Riley, Wells, 2010: 365).

In order to prevent most instances of falsified hours and salary schemes, payroll preparation, approval, disbursement, distribution and reconciliation functions should be strictly segregated. Policy, requiring a supervisor's approval of overtime work, pay changes, sick leave and vacation time, should be in place as well. In addition, maintaining restricted access to employee time sheets can prevent false alterations of hours worked (Kranacher, Riley, Wells, 2010: 365; Wells, 2011: 239; Bragg, 2009: 203). Table 2 sums up the red flags associated with the payroll schemes and methods of fraud prevention and detection.

2.2.3. Expense reimbursement schemes

Expense reimbursement schemes imply submission of a claim made by employee to

Table 2. Payroll schemes

Red flags	Prevention methods	Detection methods
▪ Paychecks for employees who: ➢ Never take a vacation ➢ Never take sick leave ➢ Have no taxes withheld ➢ Have no deductions ➢ Have no social security number ➢ Have social security number duplicated by another employee ➢ Have no physical address ➢ Have an address duplicated by another employee ➢ Have no phone number ➢ Have a duplicate phone number ➢ Have a duplicate bank account ➢ Have a date of paycheck after termination ▪ Persons on the payroll who have no personnel file ▪ Unexplained or unusual increase in wages expense/ commission expenses ▪ Commission expenses increase as a percentage of total sales ▪ Amount of uncollected sales/commissions/overtime generated by one employee is inordinately bigger compared to the coworkers ▪ Fictitious/overstated sales ▪ Mismatch in rates of pay/ hours worked data ▪ Variations from budgeted expenses	▪ Background and reference checks before hiring ▪ Segregation of duties between hiring, payroll preparation, approval, disbursement, distribution and reconciliation ▪ Restricted access to the payroll and personnel files ▪ Policy requiring a supervisor's approval of overtime work, pay changes, sick leave and vacation time	▪ Examination of payroll files ▪ Trend analysis ▪ Reconciliation of employees in the payroll database with employees in the human resources database ▪ Analyzing correlation between sales figures and commission expenses ▪ Comparative analysis of uncollected sales/ commissions/overtime generated by employee ▪ Getting independent confirmation of sales from customers ▪ Comparing rates/hours paid with rates/hours stored in the personnel files ▪ Comparing payroll expenses with budget projections

reimburse expenses that are in fact fictitious or inflated (ACFE, 2012: 12). Companies usually reimburse expenses related to business travel, lodging and meals. Expense reimbursement typically implies the following process: an employee submits a report

detailing an expense together with the support documentation for the expense (e.g., receipt); a supervisor approves the report in order for the expense to be reimbursed (Kranacher, Riley, Wells, 2010: 371). Expense reimbursement schemes include mischaracterized expense reimbursements, overstated expense reimbursements, fictitious expense reimbursements, and multiple reimbursements (ACFE, 2012: 7).

Mischaracterized expense reimbursement scheme occurs when an employee requests reimbursement for a personal, not business-related, expense. For instance, dinner with a friend is claimed as "business development". The fraudster submits the expense report, providing business purpose for the incurred cost, but attaches the receipt from the personal spending. In this case, the false document makes a victim company reimburse the employee for the personal expense (Kranacher, Riley, Wells, 2010: 371; ACFE, 2007: 1.569).

To prevent the scheme, a company should implement and enforce policy requiring the submission of detailed expense reports. Each document should describe the business purpose for the expense, time, date, location in which it incurred and exact amount. A simple review of the paper can reveal travel locations that are not known for business purposes. Also a comparison between the employee's expense reports and the work schedule can expose whether "business" expenses coincide with a vacation or day off (ACFE, 2007: 1.569, 1.571; Vona, 2008: 139).

Overstated expense reimbursement scheme commonly implies altering the price shown on the support documentation and submitting it along with the expense report. By changing the amount of expense to a higher one, an employee can pocket the difference. If the company policy does not require the original documents as support, the perpetrator can submit a photocopy to hide alterations (ACFE, 2007: 1.571).

According to the scheme's description, the fraud indicator involves altered support documentation, which can be concealed through the submission of photocopies. Obviously, to prevent the fraud, an employer should implement and enforce policy requiring original support documents to be attached to the expense report. In this case,

alterations can be detected through the detailed review of the documentation (ACFE, 2007: 1.573, 1.577).

Fictitious expense reimbursement scheme occurs when an employee "creates" business expenses that need to be reimbursed. There are several ways to generate a reimbursement for non-existed spending. One can make fraudulent support documents, e.g., counterfeit receipt printed out at home. The perpetrator can also obtain blank receipts from legitimate vendors, e.g., waiters, or steal them. One more way to conduct the scheme implies submission of the reports for expenses that were paid by others. All these manipulations cause a victim company to reimburse the perpetrator for business expenses not actually existed (Kranacher, Riley, Wells, 2010: 375).

Submission of sequentially numbered receipts, as well as receipts that are missing logical information might be a red flag of the scheme, since the fraud involves creation of fictitious support documentation. A detailed review of receipts sorted by employee and receipt number can detect such kind of anomaly (Seidler, 2011; Vona, 2008: 141). As before, to prevent the scheme, policy requiring original support documents to be attached to expense reports should be implemented and enforced (Wells, 2011: 236).

Multiple reimbursements scheme involves submission of the same expense several times. The most common way to commit the fraud is to present various types of support documents for a single expense (Kranacher, Riley, Wells, 2010: 377). If the company allows photocopies for expense items, the perpetrator might simply submit several copies of the same support document to receive multiple reimbursements (ACFE, 2007: 1.577). In some cases, when two or more employees share expenses, each one might claim for reimbursement for the same expense (Vona, 2008: 140).

According to the scheme's description, the same expense claimed on multiple reports might represent a red flag. Therefore, a review of expense reports submitted by one employee can reveal the fraud (Goldmann, Kaufman, 2009: 84). Prohibiting photocopies and allowing only original documents as support can restrict the variety of manipulations. By implementing and enforcing policy that requires the claims to be

made within a specified time period, an employer can prevent multiple submission of expense (ACFE, 2007: 1.573, 1.577).

Besides specific red flags attached to each type of the scheme, there are anomalies that can be caused by any of the expense reimbursement frauds. They include variations from budgeted expenses and unexplained or unusual increase in expense reimbursements (Wells, 2003). Such anomalies can be detected through expense account review, which involves trend analysis and comparisons with budgeted amounts, i.e., comparisons between actual and estimated expenses (ACFE, 2007: 1.577). At the same time, tracking down expense reimbursements gained by each employee allows to uncover if one has significantly bigger amount of these reimbursements compared to the coworkers.

As for the fraud prevention, the basic control is segregation of duties between preparing expense reports, approving expense amounts and issuing related payments (Kimmel, Weygandt, Kieso, 2011: 343; Wells, 2011: 239). Another prevention measure is having restricted access to the approved expense reports, so that the employees who originally submitted the documents would not have further access to them (Bragg, 2011). Table 3 recapitulates the red flags associated with the expense reimbursement schemes and methods of fraud prevention and detection.

2.3. Asset misappropriation prevention and detection in Russian small business environment

After examining billing, payroll and expense reimbursement schemes, highlighting anomalies caused by violations in question and defining fraud prevention and detection policies and procedures, the next step of the research is to put together the findings obtained from the literature and apply them in Russian small business environment. For this purpose, similar anti-fraud measures are combined and presented under either preventive or detective category. Whether a control belongs to one of the categories

Table 3. Expense reimbursement schemes

Red flags	Prevention methods	Detection methods
▪ Travel expense claims to locations that are not known for business purposes ▪ Expense claims for days when the employee had a vacation or day off ▪ Altered support documentation ▪ Consecutively numbered receipts ▪ Receipts that are missing logical information ▪ Same expense is claimed on multiple reports ▪ Unexplained or unusual increase in expense reimbursements ▪ Variations from budgeted expenses ▪ Amount of expense reimbursements gained by one employee is inordinately bigger compared to the coworkers	▪ Policy whereby detailed expense reports are submitted with the original support documentation ▪ Policy requiring the claims to be made within a specified time period ▪ Restricted access to the approved expense reports ▪ Segregation of duties between preparing expense reports, approving expense amounts and issuing related payments	▪ Detailed review of expense reports and support documentation ▪ Comparing the employee's expense reports to the work schedule ▪ Sorting receipts by employee and receipt number ▪ Trend analysis ▪ Comparing expenses with budgeted amounts ▪ Comparative analysis of expense reimbursements gained by employee

depends on the type of transactional event and where/how the control is initiated. Some detection procedures, if known to the relevant constituency, can take on preventive characteristics. For example, stock-taking is fundamentally detective control, as it is designed to reveal inventory discrepancy. However, when it is known that the procedure is conducted on a regular basis, it can also serve to prevent an unauthorized event (Bizzell, Clinton, Prentice, Stone, 2011: 22; Hightower, 2008: 44).

In the research, anti-fraud measures are classified in the following way: preventive measures include practices attempted to stop irregularities from occurring; detective measures include procedures designed to identify anomalies in business. The final list of defense practices suggested by fraud literature (Goldmann, Kaufman, 2009; Goldmann 2010; Vona, 2008; 2011; Kranacher, Riley, Wells, 2010; Wells, 2001; 2002; 2003; 2007; 2011; Coenen, 2008; 2009; Singleton, Singleton, 2010; ACFE, 2007; 2012;

Albrecht, Albrecht, Albrecht, Zimbelman, 2011; Johnson, Rudesill, 2001; Bierstaker, Brody, Pacini, 2006) is presented below:

1. *Background and reference checks before hiring* refer to looking into criminal records, checking credit reports, verifying educational credentials and contacting prior employer (Goldmann, 2010: 87-88). Such safeguard not only ensures that the person hired is trustworthy, qualified and fits for the position, but also eliminates the possibility of adding a ghost employee to the payroll.

2. *Maintaining and regularly updating an approved vendor list* assists in keeping information of all company's active vendors.

3. *Verifying entity's legitimacy before adding a new vendor to the approved vendor list* assures that the entity in question is a bona fide company (Coenen, 2009: 123). Verification can be done, for instance, by looking up a company in telephone directories, obtaining its corporate records, visiting the address on file, etc. If a list of vendors is not in place, entity's legitimacy can be checked before actual purchasing.

4. *Segregation of duties* assures that different individuals are responsible for related activities. The key principle of the control is to separate the custodial, recording/reconciling, and approval functions throughout the company (Coenen, 2008: 154). Such practice assists in reducing the temptation for an employee to commit a dishonest act.

5. *Restricted access to business records* assures that only authorized persons have access to specific data. The safeguard can be implemented, for instance, through the use of login information to enter the system.

6. *Records management policy* defines requirements for creating, processing and storing documents. In other words, the control assures that documents contain all the information needed to properly record and authorize the transaction, and are entered into the system as quickly as possible.

7. *Use of authorization* refers to establishing specific levels of authority, indicating who is permitted to initiate, approve and record transactions (Coenen, 2008: 155; Goldmann, Kaufman, 2009: 50). In the context of fraud prevention, the control is defined as a policy whereby authorized by level or position individuals sign off on transactions either by putting a signature on a paper or through the use of digital approval.

8. *Setting spending limits* assures that disbursements will not go beyond the budgeted amounts (Bragg, 2009: 28-29).

Although some fraud experts (e.g., Singleton, Singleton, 2010; Goldmann, 2010; Wells, 2011; Coenen, 2008; ACFE, 2012) consider rotation of duties as a potentially good fraud prevention measure, the procedure has received the lowest rating of effectiveness in the survey by Bierstaker, Brody and Pacini (2006). Moreover, rotation of duties may be impractical for small businesses, as it takes resources that entities may not have to educate and train staff for the new tasks.

Besides methods aimed to prevent the specific fraud schemes, there are few general cost-effective mechanisms that can be employed by small businesses. According to ACFE (2012), *a code of conduct*, *employee training programs* and *fraud hotlines* can be carried out at marginal costs in the organizations and can significantly increase prevention of fraud. In other words, by setting the bar for employee standards, educating staff on how to define and report illegal activities, and implementing an anonymous and confidential system to receive tips, small entity with limited resources can minimize the impact of fraud (Tysiac, 2012). Therefore, above-mentioned measures are included in the final list of defense practices.

Procedures aimed at revealing fraud indicators are as follows:

1. *A stock-taking* assures that the physical quantity of company's assets equals the quantity in the books. For the purpose of detecting billing frauds, the procedure is

applied to inventory and fixed asset items. According to Russian Accounting Standards (RAS), the term inventory is addressed to assets:

- used as materials, components, etc. in manufacturing products intended for sale (works, services);
- intended for sale;
- used for administrative needs of the entity[24].

In its turn, fixed assets include buildings, operating and power machines and equipment, measuring and control devices and equipment, computers, vehicles, tools, and many other objects intended for the use in product manufacturing, work performance or service provision, and for administrative needs of the organization[25].

2. *Sorting documents* refers to putting documents in a specific order. The procedure helps to detect red flags associated with false documentation.

3. *Detailed review of documentation* assures that data and documents are complete and valid.

4. *Comparing vendor invoices with approved vendor list* determines whether an invoice is received from an authorized vendor and whether the vendor's data on the document is correct.

Apart from invoices, Russian companies may deal with purchase orders when placing orders with vendors. Such documents represent the intention of buyer to acquire the exact goods or services from a single vendor, and contain all necessary purchase details (Deveau, Clough, 1999: 73). Therefore, by simply *comparing the purchase order against the invoice and against the shipping documents*, an employer can ascertain whether a transaction is valid (Goldmann, 2010: 102).

[24] In Russia, accounting of inventory is regulated by Order of the Ministry of Finance № 44n. of 09.06.2001.
[25] In Russia, accounting of fixed assets is regulated by Order of the Ministry of Finance № 26n. of 30.03.2001.

5. *Matching vendor data with employee data* determines whether there are employees posing as vendors.

6. Monitoring the nature and quantities of goods and services acquired assures that the types and quantities of purchased merchandise and services are reasonable. In this case, judgment is based on common sense and requires a good knowledge of business.

7. *Reconciliation of employees in the payroll database with employees in the human resources database* shows if nonexistent employees or retaining terminated employees are presented on the payroll.

8. *Verifying the rates of pay in a pay period or for an employee over pay periods* determines whether unauthorized rate changes are put on the payroll. At the same time, *verification of hours worked* shows if false hours are paid to an individual.

9. *Analytical review* evaluates financial information for the presence of unexpected relationships, unusual changes and abnormal fluctuations. The data can be analyzed with the help of the following techniques. *Trend (horizontal) analysis* identifies changes in financial data over a number of accounting periods. *Vertical analysis* shows proportion of each separate figure on a financial statement and a base figure within the statement. Such technique, if applied over a number of periods, can help reveal unusual changes in the behavior of accounts. *Comparison between actual and budgeted amounts* determines variances between actual and planned results. *Comparative analysis of results generated by unit* shows if one has unusually high results compared to others.

Limitation in the use of analytical procedures is that anomalous information in financial data does not necessarily indicate fraud and may simply require further analysis and investigation. In Russian business practice, the above-mentioned techniques are generally used under *financial and business analysis*.

When looking into billing, payroll and expense reimbursement schemes, some similarities in the red flags and anti-fraud methods can be noticed. For example, all the

above violations cause a significant increase in spending that can be uncovered by performing trend analysis. Other detection methods that can be shared include confirmation of data and budget preparation. Since billing, payroll and expense reimbursement schemes involve fictitious or overstated spending, confirming the accuracy of relevant data can reveal the violations. And if in case of payroll fraud, false commissions are detected by confirming the sales, likewise billing and expense reimbursement schemes can be uncovered by checking expenditures incurred directly with the vendors (Goldmann, Kaufman, 2009: 132). The same is true for budgets – making comparisons between actual and expected results can reveal variances inherent not only for payroll and expense reimbursement schemes, but for billing frauds as well. If payments to a vendor substantially exceed the budgeted amount, this may be a sign of a shell company or non-accomplice vendor scheme.

10. *Confirming data accuracy with partners* implies contacting customers/vendors to confirm the accuracy of payment/billing. The procedure determines whether fictitious or overstated sales/purchases take place.

11. *Comparing the employee's expense reports and enclosed supporting documents to the work schedule* allows to reveal whether the employee's expenses occurred during vacation or day off.

2.4. Theory summary

Theoretical findings of the current study are shown in the Figure 3 that illustrates the relationship between examined fraud concepts. The triangle in the figure represents fraud conditions. When all three conditions are met, it is an opportunity to commit and conceal the dishonest act that leads up to the variety of crimes occurred inside the organization. Depending on the state of company's internal controls, management oversight, and/or one's position and authority, a perpetrator conducts the fraud scheme that he/she believes can not be detected under given conditions. Since pressure and rationalization are individual for each person, it may be difficult for management to do

anything about an employee's needs or personal code of ethics. Therefore, business owners and executives should concentrate organization's resources on reducing opportunity - the element that is manipulated the most - by building processes, procedures and controls that prevent insiders from committing fraud and that effectively detect illegal activity if it occurs.

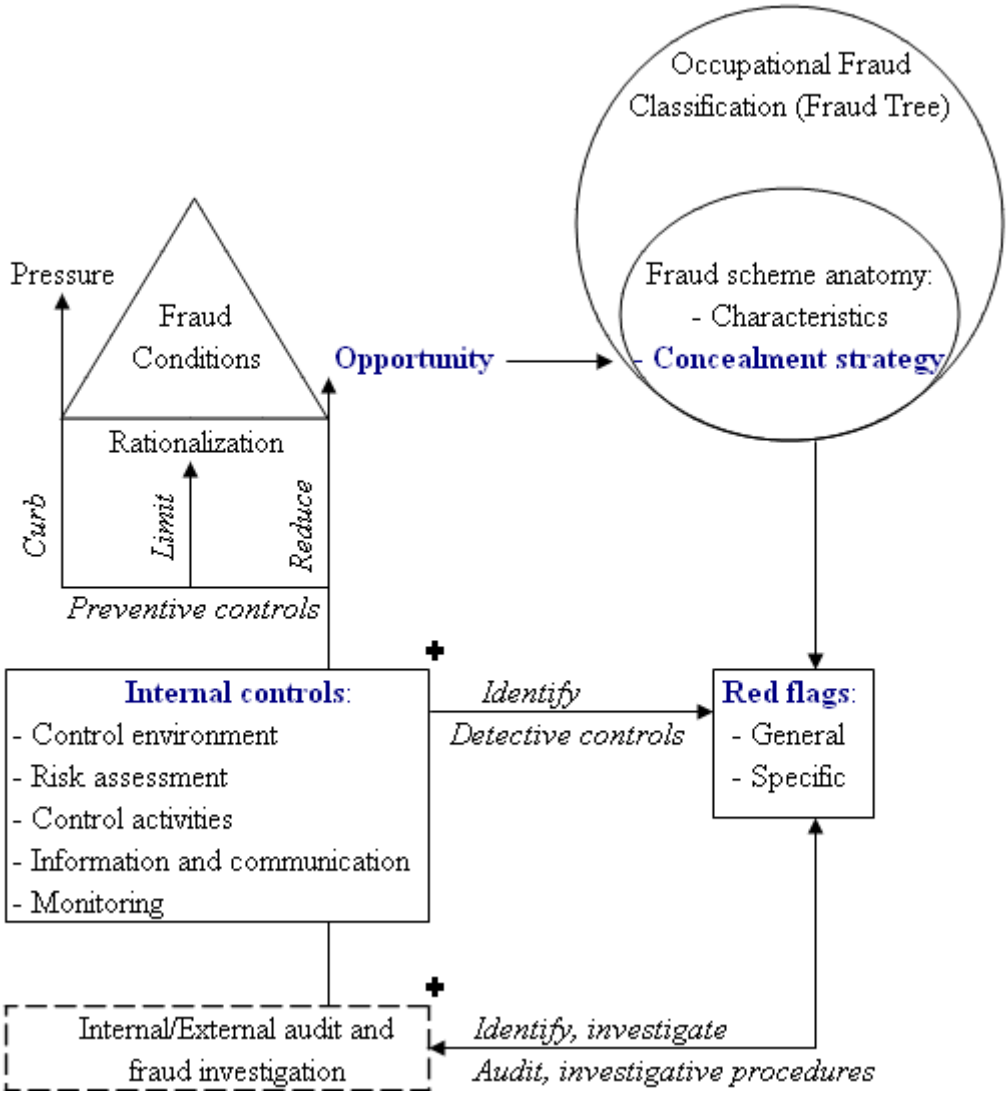

Figure 3. Fraud, its prevention and detection

When a fraudster perpetrates crime, he/she usually leaves traces of concealed dishonest act. Such traces can be identified by means of controls established by management, tests conducted by auditors and other sources both internally and externally. However, the presence of red flags does not necessarily mean that fraud takes place, and can be

provoked by non-fraud factors. Therefore, analysis of indicators is performed to determine whether signals observed are sufficient to recommend an investigation. In case investigation is conducted, the extended procedures are applied to ascertain whether fraud, as suggested by the indicators, has occurred.

Since some businesses lack an internal audit department and/or the resources to elaborate a strong set of internal controls, the focus of the research is put on the anti-fraud program that management can establish to minimize the occurrence of fraud and increase the probability of its detection. Fraud issues are examined in the context of Russian small organizations, as economic crime, particularly asset misappropriation, is the great concern for such entities. Findings on the prevention and detection of the most common violations are illustrated in the Figure 4.

Maintaining and updating an approved vendor list, segregation of duties, records management policy, code of conduct, etc. are examples of defense practices that can be utilized to manipulate the opportunity element of the fraud triangle. Additionally, design and implementation of the code of conduct can help limit other two fraud factors: employee's ability to rationalize illegal activities by explaining organization's principles and incentive to commit fraud by prompting a consideration of consequences. The employment of such prevention measures provides certain protection against white-collar crime for a small enterprise.

Audit procedures, e.g., stock-taking, employee reconciliation, document sorting, etc., are aimed at discovering the signs of asset misappropriation schemes. At the same time, the measures contribute to fraud deterrence by creating perception of detection. When the red flags are identified, either internal or external investigation is performed, followed by law enforcement and other segments of the criminal justice system that bring fraud perpetrator before the court.

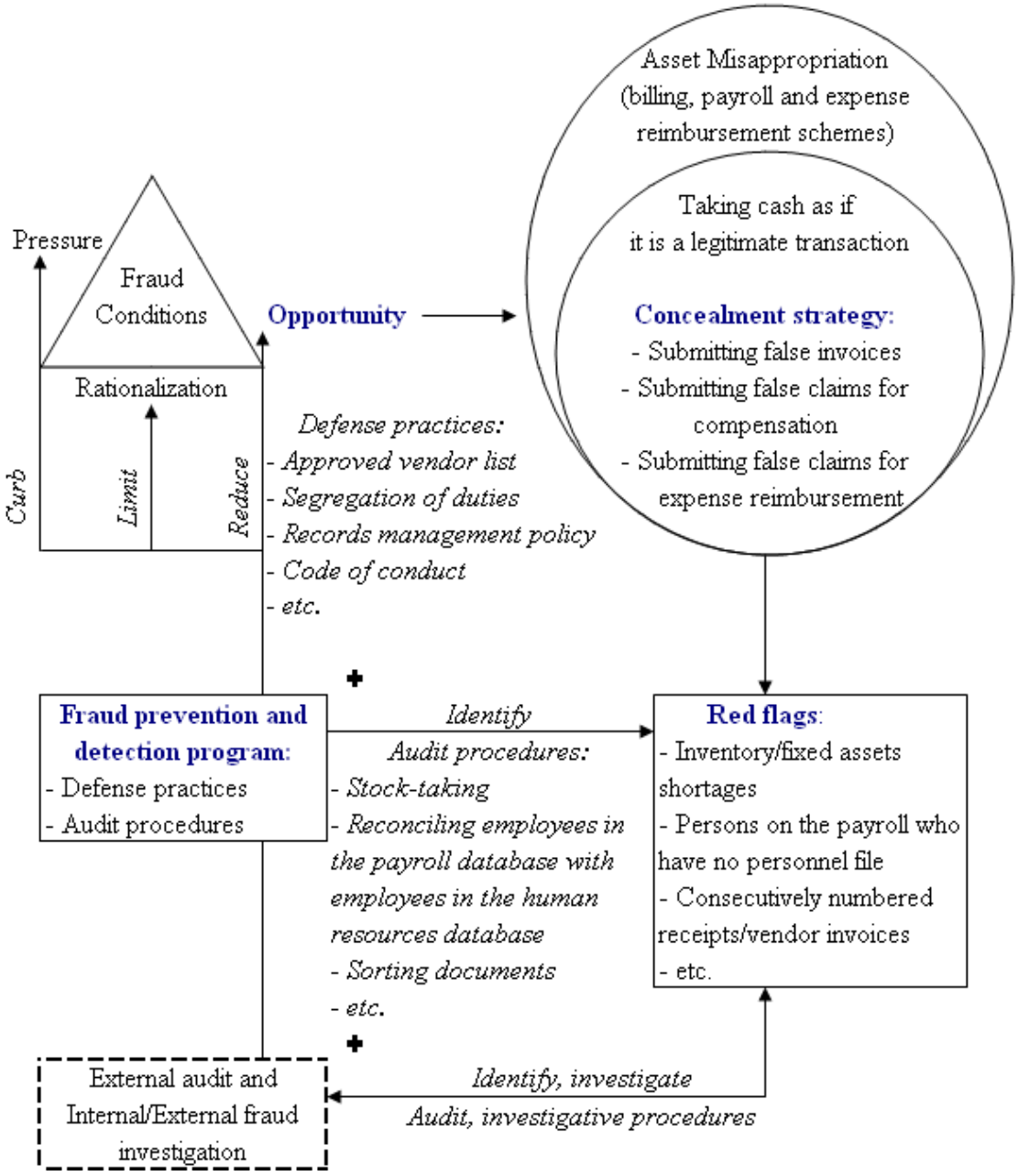

Figure 4. Billing, payroll and expense reimbursement schemes, their prevention and detection in Russian small businesses

3. METHODOLOGY

The objective of this part is to justify and explain the choice of research methods used in the context of the research problem. The chapter presents the research design, a description of the sample, reliability and validity estimation.

3.1. Research design

For the purpose of answering the research question, a descriptive study is initiated to determine accountants' and managers' personal and subjective perceptions regarding effectiveness of anti-fraud policies and procedures. In this work, descriptive design is used to discover the characteristics of a given population, not to test theory. The paper reports on the current state of anti-fraud measures usage in Russian small businesses and presents summary data on effectiveness of the measures in preventing and detecting white-collar crime. Additionally, comparison between accountants' and managers' responses is made, and difference in their opinions is identified.

The study uses both qualitative and quantitative approaches to research. Analysis of written materials provides qualitative information on the fraud issues, which is later used in the questionnaire to find out details on the topic in the given context. Thereafter, quantitative value is ascribed to qualitative data to make it amenable to further analysis. By adopting a combination of qualitative and quantitative approaches, the study provides precise and testable expression to qualitative ideas.

3.1.1. Content (conceptual) analysis[26]

The purpose of conducting content (conceptual) analysis is to answer the research sub-question 1: *what measures do fraud experts recommend to prevent and detect billing, payroll and expense reimbursement schemes?* In this connection, fraud literature is

[26] http://writing.colostate.edu/guides/page.cfm?pageid=1309

reviewed for the presence of fraud prevention and detection measures. In particular, articles, books and other papers on corporate fraud, fraud auditing and investigation, and forensic accounting are scrutinized to determine defense practices and audit procedures aimed to combat billing, payroll and expense reimbursement schemes (see Table 4).

The content analysis is performed in the following way[27]. Each red flag and associated detection method found in the work of one fraud expert is tested for the presence in the works of other authors. If either a red flag or detection method is missing in one publication, it is searched, at first, among other works of the same author, and then, if it is not found, in the works of other authors. The same procedure is conducted in respect to prevention methods.

Whether a measure is applicable for the further research depends on how many times it is mentioned by different fraud experts. For the purpose of creating an extensive list of anti-fraud methods, the chosen frequency equals to 3, meaning that at least 3 authors have mentioned the method either independently or in collaboration. After such a selection, anti-fraud measures are checked for the usability in Russian small businesses by eliminating complex practices and procedures and focusing on those that can be performed on a regular basis as a part of employee duties. Thereafter, the paper examines which of the remained methods work "the best". The results of the content analysis are presented in the paragraph 2.3 of the thesis.

3.1.2. Survey design

Due to the need for information on the effectiveness of fraud prevention and detection methods that could be applied in small businesses, a survey-based research is conducted to build a database for analytical purposes. In particular, the study describes how

[27] The coding choices are made with respect to the coding steps indicated by Carley (1993). In the current research, the data is coded in terms of existence in the works of different fraud experts and then later collapsed to frequencies.

Table 4. Fraud literature

Author	Title	Year
1. Johnson, Gary G., Rudesill, Charryl L.	An investigation into fraud prevention and detection of small businesses in the United States: responsibilities of auditors, managers, and business owners	2001
2. Wells, Joseph T.	Enemies Within	2001
3. Wells, Joseph T.	Billing Schemes, Part 1: Shell Companies That Don't Deliver	2002
4. Wells, Joseph T.	Billing Schemes, Part 2: Pass-Throughs	2002
5. Wells, Joseph T.	Billing Schemes, Part 3: Pay-and-Return Invoicing	2002
6. Wells, Joseph T.	Billing Schemes, Part 4: Personal Purchases	2002
7. Wells, Joseph T.	Keep Ghosts Off the Payroll	2002
8. Wells, Joseph T.	The Padding That Hurts	2003
9. Wells, Joseph T.	Protect small business	2003
10. Bierstaker, James L., Brody, Richard G., Pacini, Carl	Accountants' perceptions regarding fraud detection and prevention methods	2006
11. Association of Certified Fraud Examiners	Fraud Examiner's Manual	2007
12. Wells, Joseph T.	Fraud Casebook: Lessons from the Bad Side of Business	2007
13. Coenen, Tracy	Essentials of Corporate Fraud	2008
14. Vona, Leonard W.	Fraud Risk Assessment: Building a Fraud Audit Program	2008
15. Coenen, Tracy	Expert Fraud Investigation: A Step-by-Step Guide	2009
16. Goldmann, Peter D., Kaufman, Hilton	Anti-Fraud Risk and Control	2009
17. Goldmann, Peter D.	Financial Services Anti-Fraud Risk and Control Workbook	2010
18. Kranacher, Mary-Jo, Riley, Richard, Wells, Joseph T.	Forensic Accounting and Fraud Examination	2010
19. Singleton, Tommie W., Singleton, Aaron J.	Fraud Auditing and Forensic Accounting	2010
20. Albrecht, Conan C., Albrecht, Chad O., Albrecht, W. Steve, Zimbelman, Mark F.	Fraud Examination	2011
21. Vona, Leonard W.	The Fraud Audit: Responding to the Risk of Fraud in Core Business Systems	2011
22. Wells, Joseph T.	Corporate Fraud Handbook : Prevention and Detection	2011
23. Association of Certified Fraud Examiners	Report to the Nations on Occupational Fraud and Abuse	2012

managers and accountants perceive effectiveness of anti-fraud methods and what methods are actually used in their organizations. Next, the information is analyzed, and conclusion is made on whether the entities employ the most or the least effective techniques.

The survey method of data collection was selected due to several reasons. First, surveys are good at dealing with specific issues, when the researcher knows in advance precisely what kind of information is needed. Second, the surveys are best suited to gathering data on relatively straightforward, relatively uncomplicated facts and thoughts. Third, surveys are good at collecting information about a large number of people (Denscombe, 2010: 12). In the context of the current research problem, there is no need to conduct in-depth investigation, which is suited to really complex issues; the required information is clearly identified based on study sub-questions; it is desirable to obtain mass data on the subject to come up with reliable results.

For the purpose of this study, a cross-sectional design is used to assess availability of fraud prevention and detection methods in small businesses and gather opinions of insiders on their effectiveness at a single point in time. In other words, data collection occurred only once. Longitudinal design was not applied, as the research agenda does not require repeatedly collected data.

Since it is practically impossible to measure the entire target population, a sample survey is conducted to obtain information of sufficient quality in a fast and economic way. In particular, convenience sampling was applied to question subjects that are close to hand. Regardless of the fact that convenience samples facilitate easy, inexpensive and fast data collection, they carry possible bias and limits on generalization of the results, due to non-random manner of selection (Krishnaswami, Satyaprasad, 2010: 53, 56). And though it is difficult to make inferences about the population, while using such a subjective method of selection, the current research can serve as a basis for further extensive survey. In this case, convenience sampling can be useful for gaining rough impression about the subject of interest.

In order to obtain data on a research subject, questionnaires are allocated among managers and accountants. One of the advantages of using a questionnaire is comparability of collected data between different respondent groups and over the course of time. Also, it is cost-effective, quick and well suited to extracting information from a large number of people (Kaptein, Avelino, 2005). The disadvantage is that the researcher may never know if the respondent understood the question that was being asked. Additionally, questionnaires may produce very low return rates, whether they are mail or online questionnaires (Krishnaswami, Satyaprasad, 2010: 121; McDonald, Adam, 2003).

The current research questionnaire consists of two individual parts. The first part includes questions aimed at obtaining demographic information on the respondents. The second part examines managers' and accountants' perceptions regarding effectiveness of anti-fraud measures and includes a rating scale to determine the prevalence of respondents' opinions. Responses range from "completely ineffective" to "completely effective" with seven total answer options. Each option is assigned a score (1 = completely ineffective to 7 = completely effective), and these scores are used in survey response analysis. The research on the reliability and validity of scale scores suggests that the optimal number of response categories in rating scales lies between 7 and 10 options (Preston, Colman, 2000).

In order to encourage people to answer questions about themselves and give their opinions, a brief statement, explaining the purpose of the survey and reassuring about the anonymity of the obtained information, is presented at the top of the questionnaire. Also, fraud-related terms are explained, and interpretation of anti-fraud measures is provided to ensure that the collected responses are valid.

Both parts of the questionnaire are first developed in English and then translated to Russian. These versions are compared and some changes are made. To check the relevance and the construct of the survey instrument, it is tested by having one senior accountant and one senior manager review and fill in the questionnaire before it is distributed to the sample. As a result, some modifications in the wording are made. Both

English and Russian versions of the questionnaire are presented in Appendix 3 and Appendix 4 respectively. The average time required for a respondent to complete the survey is about ten minutes, which is both adequate to the data collection objectives and fast enough to avoid potential respondent's loosing interest due to an excessive demand of their time.

Distribution of the questionnaire is made though the use of electronic mail, most commonly referred to as e-mail, which is relatively fast and inexpensive alternative to the post (McDonald, Adam, 2003). At the same time, it can be fast and easy secondary distribution based on an appropriate request in the message for forwarding to other potential respondents (Bonometti, Tang, 2006). Additionally, e-mail surveys code the data automatically, eliminating the hand-coding, and therefore save the researcher time and resources (Cobanoglu, Warde, Moreo, 2001).

The current survey is conducted by sending the questionnaire as an attachment in an e-mail. The main advantage of this method is the ability to give to the questionnaire a format and appearance that will be inviting and pleasing to the research participants (Gunter, Nicholas, Huntington, Williams, 2002).

The limitation of electronic survey is that some people may be quite selective when reading their e-mails and, as a result, may ignore certain types of e-mails considering them as "junk mail" or spam (Bonometti, Tang, 2006). It is also hard to ensure the respondents' anonymity: when individuals return questionnaires, they reveal personal identity through their e-mail addresses and network routes. Additionally, the content of response is virtually accessible by Internet intruders. The lack of anonymity could be a factor that discourages some people from participating in surveys using the new medium because of security and privacy concerns (Dommeyer, Moriarty, 1999; Ranchhod, Zhou, 2001). Another drawback involves the use of e-mail attachments that are associated with the risk of introducing computer viruses. If the potential respondent fears getting a virus from downloaded files, he/she may be reluctant to take part in the study (Dommeyer, Moriarty, 1999; Gunter, Nicholas, Huntington, Williams, 2002). The

lack of tangible incentives via electronic surveys is also seen as one of the limitations of using this method (Ranchhod, Zhou, 2001).

In order to increase the response rate and speed to e-mail study (Sheehan, Hoy, 1999; Sheehan, 2001), survey invitation and follow-up message are sent to potential participants. Survey invitation used in this research is presented both in English and Russian in Appendix 1 and Appendix 2 respectively. The first e-mail is sent in June 2013. It includes a short letter, disclosing information about the research, and two attachments. The main objective of the letter is to motivate recipients to participate in the survey. The recipients are asked to respond to the questionnaire within one week. Reminder message (similar to that in Appendix 1 and Appendix 2) is sent to those who have not answered within the given time. The recipients are asked again to respond to the questionnaire within one week.

Originally, the questionnaire is constructed in DOC format. In order to simplify its filling, check boxes are implemented, allowing the respondents to mark options within the Word document. A PDF format of the questionnaire is also attached to the e-mail, in case someone is experiencing difficulties in using check box instrument or having a word processor that can not "read" the DOC file. Three recipients used this option and returned the questionnaire by attaching the scanned document to an e-mail reply.

3.2. Sample

The sample of the current research is represented by accountants and managers of Russian small businesses – organizations with less than 100 employees. In total, 14 business practitioners (7 accountants and 7 managers) participated in the study. In an attempt to obtain sufficient for analysis amount of data in a short time, multiple techniques were used to get into touch with the potential respondents. Thus, nine survey participants were found through the private contacts within Russian social network (vk.com/). Five practitioners were reached through the initial respondents, meaning that questionnaire was forwarded further by individuals to others from the target population.

Seventy-one percent of the survey participants hold a specialist's degree, twenty-nine percent have a master's degree. 57 percent work at organizations with 1-15 employees, 43 percent work at organizations with 16-50 employees. Practitioners come from different industries, such as manufacturing (29 percent), construction (29 percent), wholesale and retail trade (29 percent) and services (13 percent). Overall, respondents are diverse in terms of age, years of experience, organization size and industry. A summary of these results is presented in Table 5.

Table 5. Demographic data

	Number of respondents	Percentage
Respondent's occupation:		
Accountant	7	50
Manager	7	50
Respondent's age:		
25 to 34 years	12	86
45 to 55 years	1	7
above 55 years	1	7
Respondent's educational level:		
Specialist's degree	10	71
Master's degree	4	29
Respondent's experience in occupation:		
0 to 4 years	7	50
5 to 9 years	5	36
10 to14 years	1	7
more than 20 years	1	7
Main business activity:		
Manufacturing	4	29
Wholesale and retail trade	4	29
Construction	4	29
Services	2	13
Organization size:		
1-15 persons	8	57
16-50 persons	6	43

Overall, 12 organizations were examined for the presence of anti-fraud methods. Because of small organization size, only the most appropriate contact person was selected from each entity. In 11 organizations either manager or accountant participated in the survey. In 1 organization 3 managers responded to the questionnaire. The reason for inquiring multiple managers lied in the diversity and complexity of the entity's operations.

The survey response rate comprises 100 %, meaning that all recipients agreed to participate in the study and returned the questionnaire. Moreover, all responses appeared to be usable for analysis. The research does not have any missing values due to response examination straight after the questionnaire is returned. If missing data is noticed, the recipient is contacted and asked to provide necessary information promptly.

The primary selection criterion, which was used to form a sample for the research, involved an easy access to each potential respondent by e-mail or through the social network. Due to the fact that private contacts with managers and accountants were established mainly in Saint-Petersburg educational institutions, the majority of the study participants had limited working experience at the time of conducting the survey. Thus, the research sample restricts the inclusion of the potential respondents with more years of practice. Moreover, the current selection does not contain organizations with 51-100 persons in staff and therefore, there is no evidence on the use of anti-fraud measures in such entities.

It is possible that more experienced managers and accountants who were left out during the selection process might have different perception regarding effectiveness of fraud prevention and detection measures. As a result, their responses might affect the study outcome. Indeed, Johnson and Rudesill (2001) in their work indicated that experience is an influencing factor in how accountants rate the effectiveness of certain defense practices. Thus, there is a risk that data received from the less experienced survey participants might differ from those given by individuals with more years of practice. Additionally, organizations with 51-100 employees, due to larger size, might have more safeguards in place as compared to the examined entities. All this leads to the

proposition that there might be a difference between the results from the current study and the results from the entire population.

3.3. Reliability and validity

The important aspects of the accuracy of the results are reliability and validity. In order to ensure reliability of managers' and accountants' answers, the questionnaire is self-administered and all respondents receive similar questions which are tested for wording. Additionally, close-ended questions are utilized to provide survey participants with a set number of options. At the same time, a Likert scale, intended to measure respondents' opinions, ensures the easiness of answering.

The validity of the results is achieved by questioning managers and accountants about known anti-fraud measures. The data received from respondents is well matched to the research question of the study, as it bears the scores that are later used to conclude on the most effective and ineffective fraud prevention and detection techniques. Additionally, the questionnaire provides an explanation of the basic fraud terminology and interpretation of defense practices and audit procedures. Such information reduces the possibility of an incorrect understanding of the questions by respondents. Moreover, to make managers and accountants perceive the survey as non-threatening and thus, enhance validity of their answers, the results of the study are interpreted on a general level to guarantee the anonymity of any individual organization. The use of optimal number of response categories (i.e., 7 options) in a Likert scale also positively affects validity.

4. RESULTS OF THE SURVEY

The objective of this part is to summarize and interpret data in a way that provides a clear answer to research question.

4.1. Use and effectiveness of fraud prevention and detection methods

Based on the fraud literature review (see Table 4 for a list of references), accountants and managers were asked to indicate whether their organizations used the following defense practices: restricted access to business records, spending limits, records management policy, approved vendor list, vendor's legitimacy verification, segregation of duties, authorization for transactions, code of conduct, background and reference checks, fraud hotline, fraud detection training (see Table 6 for data on the frequency usage of the safeguards). In addition, respondents were asked to rate the effectiveness of these measures in preventing fraud on a scale from 1 (completely ineffective) to 7 (completely effective). Figure 5 presents the results.

Table 6. Use of fraud prevention methods

N	Fraud prevention methods	Frequency, %
1	Restricted access to business records	75
2	Setting spending limits	67
3	Records management policy	67
4	Maintaining an approved vendor list	58
5	Verifying vendor's legitimacy	58
6	Segregation of duties	58
7	Use of authorization	50
8	Code of conduct	42
9	Background and reference checks before hiring	33
10	Educating staff on fraud detection	17
11	Fraud hotline	8

To sum up the effectiveness scores assigned by survey participants, mean and standard deviation are applied. The mean is computed as the sum of all the observed outcomes from the research sample divided by the total number of events. Thus, it helps identify where the center of the data set is. One problem with using the mean is that it can be strongly affected by an outlier[28]. Therefore, the population standard deviation is used to determine the amount of dispersion of data for those who participated in the study. Since the research sample is non-random, statistical analysis can not be conducted. Hence, sample standard deviation is not computed.

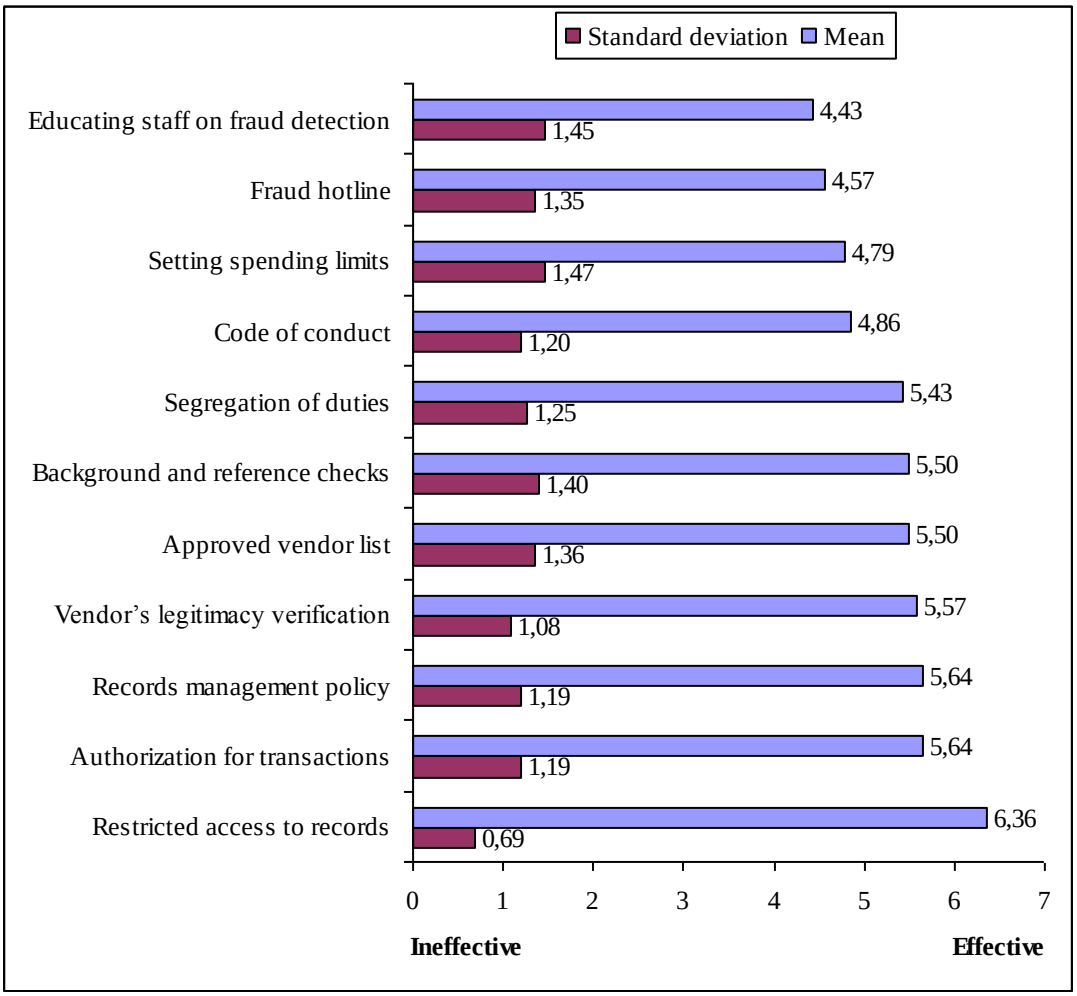

Figure 5. Effectiveness of fraud prevention methods

As shown in Table 6, the most frequently used defense practices are restricted access to business records (75 percent), spending limits (67 percent) and records management

[28] Outcome that is very far from the rest of the data.

policy (67 percent), while the least frequently used are fraud hotline (8 percent) and fraud detection training (17 percent). Meanwhile, according to Figure 5, respondents rated having restricted access to business records in organization as the practice most effective in preventing fraud, with a mean score of 6.36 and standard deviation of 0.69. This finding is similar to that presented in the work of Johnson and Rudesill (2001), where controlled access to assets and records was among the most effective fraud prevention measures. At the same time, fraud detection training received the lowest mean value of 4.43 with the standard deviation of 1.45 and thus, was rated by survey participants as the practice least effective in preventing illegal activities. However, Andi McNeal, the ACFE's director of 2012 research, highly recommended this technique (see Tysiac, 2012), stating that "if done properly, anti-fraud training program can save an organization lots of resources both in the short and the long run".

Interestingly, the most frequently met among examined entities defense practice received the highest rating of effectiveness, while one of the least frequently met received the lowest rating of effectiveness. One explanation for this might be that accountants and managers have more confidence in the practices, in which they are involved, than in those they did not have a chance to apply and therefore, form a definite opinion on. As to the perceptions of different respondent groups, accountants agree with managers that having restricted access to business records is the most effective fraud prevention measure. However, managers in this study gave the lowest rating of effectiveness to confidential employee fraud hotline, while accountants considered fraud detection training as the least effective defense.

Based on the fraud literature review (see Table 4 for a list of references), survey participants were asked to indicate whether their organizations used the following audit procedures: sorting documents, data confirmation with vendors/customers, review of documentation, comparing the purchase order against the invoice and against the shipping documents, monitoring the nature and quantities of goods and services, comparing expense reports and enclosed supporting documents to the work schedule, comparing vendor invoices with approved vendor list, stock-taking of inventory and/or fixed asset items, financial and business analysis, matching vendor data with employee

data, reconciliation of employees in the payroll database with employees in the human resources database, hours worked and/or the rates of pay verification (see Table 7 for data on the frequency usage of procedures). In addition, accountants and managers were asked to rate the effectiveness of these measures in detecting fraud on a scale from 1 (completely ineffective) to 7 (completely effective). Figure 6 summarizes the results.

Table 7. Use of fraud detection methods

N	Fraud detection methods	Frequency, %
1	Sorting documents	100
2	Data confirmation with vendors/customers	100
3	Review of documentation	92
4	Comparing the purchase order against the invoice and against the shipping documents	83
5	Monitoring the nature and quantities of goods and services	83
6	Comparing expense reports and enclosed supporting documents to the work schedule	83
7	Comparing vendor invoices with approved vendor list	75
8	Stock-taking of inventory and/or fixed asset items	75
9	Financial and business analysis	75
10	Matching vendor data with employee data	58
11	Reconciliation of employees in the payroll database with employees in the human resources database	58
12	Hours worked and/or the rates of pay verification	50

As shown in Table 7 and Figure 6, hours worked and/or the rates of pay verification is the least frequently used among examined entities audit procedure (50 percent), with considerably low mean effectiveness rating of 5.36 and standard deviation of 1.11. Detection procedures, such as sorting documents and data confirmation with vendors/customers, were implemented in all participants' organizations (100 percent). At the same time, both measures received a high effectiveness rating, with a mean of 6.00 and 6.29 and standard deviation of 1.00 and 0.80 respectively.

Respondents rated comparing purchase order with invoice and with shipping documents and confirming data with vendors/customers as the most effective. Ranked least effective was matching vendor data with employee data. Interestingly, stock-taking

procedure did not receive very high effectiveness score in the current research. However, in the work of Johnson and Rudesill (2001), testing physical inventory was rated as one of the most effective.

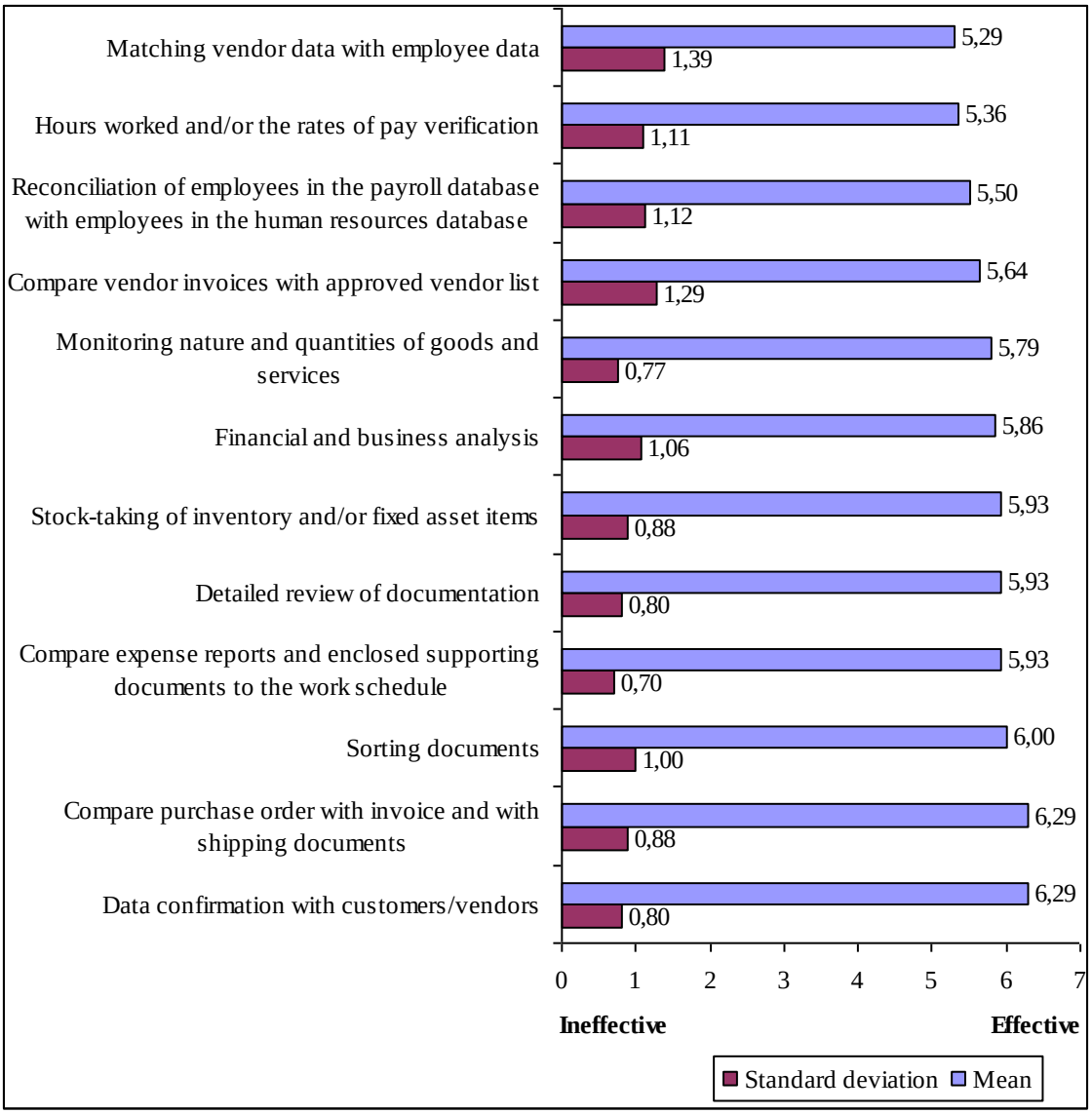

Figure 6. Effectiveness of fraud detection methods

Overall, audit procedures that are frequently met in organizations received high ratings of effectiveness, while measures that are not so common in small businesses received low ratings of effectiveness. As to the perceptions of different respondent groups, managers and accountants agree on giving high effectiveness rating to the procedures, such as confirming data with customers/vendors and comparing purchase order with

invoice and with shipping documents. However, accountants rated matching vendor data with employee data as the least effective fraud detection measure, while managers gave the same lowest effectiveness score to both employees' reconciliation and hours worked and/or the rates of pay verification procedures.

In general, respondents are more confident in fraud detection techniques than in defense practices. Also there is no significant difference in how accountants and managers perceive the overall effectiveness of anti-fraud methods listed in the study. Only few examined small-scale enterprises had sufficient amount of defense practices and audit procedures in place to protect their business from asset misappropriation schemes. Surprisingly, organizations with 1-15 employees applied fraud prevention and detection measures more frequently than organizations with 16-50 employees. Overall, audit procedures were more commonly used by small entities than defense practices.

To sum up, by describing data on the use of fraud prevention and detection methods in the examined entities, this section provides an answer to the research sub-question 2: *what measures do Russian small businesses have in place to prevent and detect billing, payroll and expense reimbursement schemes?* Additionally, the paragraph presents effectiveness ratings of fraud prevention and detection methods given by managers and accountants of small organizations and thus, responses to the research sub-question 3: *how do managers and accountants estimate effectiveness of the measures in preventing and detecting billing, payroll and expense reimbursement schemes?*

4.2. Discussion and recommendations

It was expected that small organizations would have little resources to devote to fraud prevention, thus availability of anti-fraud measures should be limited. In fact, analysis of the use of defense practices and audit procedures indicates that at the examined entities many basic safeguards were under-utilized. Thus, the current research agrees with the previous studies, such as ACFE (2012), Bierstaker, Brody and Pacini (2006), that small organizations are reluctant to invest in anti-fraud measures.

Unlike the works that focus on the costly control mechanisms, this paper is addressed to defense practices and audit procedures that provide an appropriate cost/benefit balance for small businesses. Indeed, the measures selected during literature analysis are highly recommended by fraud experts to organizations with limited resources. For instance, ACFE (2012) emphasizes the cost-effectiveness of fraud hotlines, code of conduct and anti-fraud training programs. Such measures can be easily implemented in Russian small entities at a marginal cost and can greatly increase the ability to prevent and detect fraud. Nevertheless, despite the potential effectiveness, only few examined organizations had employee training and fraud hotline in place and less then half of the organizations established code of conduct. The reason for this could be that business owners may underestimate the potential benefits of the safeguards in terms of cost savings from reduced losses related to fraud.

It is also possible that organization's management is unable to adequately implement anti-fraud measures and therefore, may doubt the necessity of such techniques in the business. As one survey participant noticed: "Implementation of certain safeguards may require additional costs. However, there is a risk that even being detected, the fraud incident will stay unreported."

Another reason, why small entities under-utilize fraud prevention and detection techniques, could lay in the nature of organization's business and complexity of the operations. For example, some service companies may not have any fixed assets in possession and may apply just-in-time inventory system (i.e., having the right material, at the right time, at the right place, and in the exact amount), thus, lacking or having a very low inventory level. In this situation, stock-taking of inventory and fixed asset items is an unnecessary procedure. Additionally, due to the small-scale of operations, some entities, particularly those with up to 15 employees, may not have certain processes, e.g., expense reimbursement. Thus, the lack of claims leaves no chance for the fraud and therefore, safeguards in this area are not required.

It is also possible that Russian small organizations have little controls in place due to friendly and trustworthy working environment. As one survey participant noticed: "In

Russia, 90% of relationship in small business is built on trust". In fact, it is common for small entities to have nepotism[29] in the workplace and as a result, under-utilize certain policies and procedures, e.g., background and reference checks. However, even if business owner prefers to hire the person recommended by a current employee, having too much trust and too little safeguards poses a threat to the welfare of small enterprise, as trust can be easily abused by a dishonest individual.

Working conditions could also be the reason for poor use of anti-fraud measures in Russian small businesses. Indeed, having employees working in one or two adjoining offices allows to stay abreast of all the conversations. Therefore, organization's management might have a perception that in such circumstances it is hard for anyone to commit and conceal illegal activities. However, numerous fraud cases described in the literature show that small businesses that do not have basic controls in place are particularly vulnerable to deception, since perpetrator can easily find a loophole in the present environment.

Because small organizations are the most in need of protection from white-collar crime, the current paper provides some recommendations on the use of basic and cost-effective fraud prevention techniques:

1. Instead of using an anonymous telephone hotline as the fraud reporting mechanism, small businesses can implement cheaper alternatives to gather information about potential fraud and other concerns. For example, a traditional suggestion box can be constructed to receive paper feedback. Another option is to create a Web form to deal with online messages.

2. Anti-fraud training program does not have to be expensive. At a minimum, staff can be educated about what constitutes fraud, what signs should alert one to the suspicious activity and how to report it.

[29] A favoritism shown by the company to the relatives or friends of the employer or the owner.

3. Organization's code of conduct can have a simple design and content. Moreover, the cost of instituting a code can be essentially limited to the expense required for the labor to implement it. The document can address the following general issues and topics: employee conduct while at work; conflicts of interest; confidentiality; relationships with customers and suppliers; unethical behavior; etc.

4. It is possible to achieve appropriate segregation of duties in organizations with a small number of employees. For example, in entities with 3 persons on staff, invoices, time sheets/salary amounts and expense reimbursement claims can be approved by business owner. Office manager can be responsible for preparing and processing documents, while accountant – for recording transactions. Payments to vendors and employees can be again arranged by business owner.

5. Before hiring an employee, small business owner or human resources manager can, at a minimum, contact a former employer. Additionally, resumes can be scrutinized and information verified to determine its legitimacy.

6. Verification of the vendor's legitimacy can be conducted by simply finding any evidence that the entity exists in reality, e.g., checking company's website for a physical address or a phone number. Additionally, one can "Google" a company to get to know more about who they really are behind the superficial image.

7. Authorization procedures should be enforced in purchase, payroll and expense reimbursement transactions. An authorization control in the purchasing area can be implemented, e.g., by having a policy that any transaction over certain amount must be approved by business owner or senior manager.

To sum up central survey results, examined Russian enterprises are not interested to invest in anti-fraud methods. This could be due to the fact that: 1) organization's management puts too much trust in employees, underestimates fraud opportunities in present conditions, has a doubt about cost-effectiveness of defense practices and audit procedures, or experiences difficulties in implementing measures in the business; 2)

organization may not need certain policies and procedures, in view of business nature and simplicity of the operations.

It was expected that small enterprises would be more likely to have cheap anti-fraud measures than expensive ones. However, the survey results show that even simple and inexpensive defense practices and audit procedures are under-utilized in such entities. This suggests that small business owners and managers may be unaware of the threat of white-collar crime or underestimate its scope and impact on the organization's welfare.

It was expected that managers' and accountants' perceptions regarding effectiveness of fraud prevention and detection methods would vary slightly due to difference in education and professional experience. In fact, the survey did not expose significant variance in respondents' estimations. Overall, anti-fraud measures received almost the same rank order of effectiveness on behalf of accounting and management practitioners. Also, these respondent groups gave pretty much the same ratings of total effectiveness of defense practices and audit procedures.

Finally, during the survey it was expected to answer the research question: *what measures are effective in preventing and detecting billing, payroll and expense reimbursement schemes in Russian small businesses?* The results of the study show that the most effective fraud prevention technique that could be used in Russian small-scale enterprises is having restricted access to business records, while the most effective fraud detection measures are data confirmation with customers/vendors and comparing purchase order with invoice and with shipping documents. At the same time, all these measures were among the most frequently met in the examined organizations. Complete information on the use and effectiveness of other anti-fraud policies and procedures is presented in the paragraph 4.1 of the thesis.

5. CONCLUSION

This study investigates the extent to which Russian small organizations use various fraud prevention and detection methods, as well as managers' and accountants' perceptions regarding their effectiveness. In particular, the research focuses on asset misappropriation schemes that pose a great threat to small businesses in Russia and presents a list of basic and inexpensive methods to combat illegal activities, which are later examined for the effectiveness and presence in the organizations.

The survey results suggest that document sorting and data confirmation with vendors/customers are the most commonly used measures to detect fraud. However, comparing the purchase order against the invoice and against the shipping documents is less often used, despite receiving the high rating of effectiveness. Meanwhile, restricted access to business records is the most frequently met preventive practice, which has also the highest ranking among anti-fraud measures. In general, defense practices and audit procedures that are commonly employed have received the high effectiveness scores. Thus, it can be concluded that although small entities have little policies and procedures in place, those that are implemented in the business are considered effective.

The research has practical implications for small business management. It provides prescriptive information on what fraud prevention and detection methods work the "best". Additionally, it suggests that some basic safeguards are not used and may be underestimated in terms of effectiveness. Small business owners and managers may wish to consider implementing effective methods, in order to prevent fraud schemes in their organizations.

The paper has some limitations. First, the findings of this study cannot be generalized beyond the examined Russian small-scale enterprises. Therefore, there is a risk that the results from the study might differ significantly with the results from the entire population. Second, new potentially effective anti-fraud measures could remain unnoticed, due to method of selection that focuses on the policies and procedures recommended by at least three fraud experts.

Taking into account the above limitations, future extensive studies may address the issues of fraud prevention and detection to Russian small- and large-scale organizations independently. Moreover, due to insufficient amount of information on behalf of Russian body of the research, statistics on the fraud incidents, perpetrators and losses due to illegal activities may be collected, in order to raise awareness of white-collar crime among Russian business owners and managers. Apart from the local surveys, future study may extensively examine fraud prevention and detection of small organizations on an international level. Additionally, future research may investigate protection of small entities from the infrequent, but costly fraud schemes.

REFERENCES

Books:

Albrecht, W. Steve, Albrecht, Chad O., Albrecht, Conan C., Zimbelman, Mark F. 2011. *Fraud Examination*. Mason: Cengage Learning.

Bizzell, Allen, Clinton, B. Douglas, Prentice, Robert A., Stone, Dan, 2011. *CPA Exam Review: Business Environment and Concepts 2011*. Sedona: Efficient learning Systems.

Bragg, Steven M. 2009. *Accounting Control Best Practices*. Hoboken: John Wiley & Sons.

Burke, Ronald J., Cooper, Cary L., Tomlinson, Edward C. 2010. *Crime and Corruption in Organizations: Why It Occurs and What to Do About It*. Farnham: Gower Pub Co.

Carmichael, Douglas R., Graham, Lynford E., Whittington, O. Ray 2007. *Accountants' Handbook*. Hoboken: John Wiley & Sons.

Coenen, Tracy L. 2008. *Essentials of Corporate Fraud*. Hoboken: Wiley.

Coenen, Tracy L. 2009. *Expert Fraud Investigation: A Step-by-Step Guide*. Hoboken: John Wiley & Sons.

Denscombe, Martyn 2010. *Good Research Guide: For small-scale social research projects*. Berkshire: McGraw-Hill Professional Publishing.

Deveau, Stephanie, Clough, Kate 1999. *Success on the Job: Writing at Work*. Portland: Walch Publishing.

Goldmann, Peter D. 2010. *Financial Services Anti-Fraud Risk and Control Workbook*. Hoboken: John Wiley & Sons.

Goldmann, Peter, Kaufman, Hilton 2009. *Anti-Fraud Risk and Control Workbook*. Hoboken: John Wiley & Sons.

Gramling, Audrey A., Johnstone, Karla M., Rittenberg, Larry Eugene 2011. *Auditing*. Mason: South-Western, Cengage Learning.

Hightower, Rose 2008. *Internal Controls Policies and Procedures*. Hoboken: John Wiley & Sons.

Kranacher, Mary-Jo, Riley, Richard, Wells, Joseph T. 2010. *Forensic Accounting and Fraud Examination*. Hoboken: Wiley.

Krishnaswami, O.R., Satyaprasad, B.G. 2010. *Business Research Methods*. Mumbai: Global Media.

Singleton, Aaron J., Singleton, Tommie W. 2010. *Fraud Auditing and Forensic Accounting*. Hoboken: Wiley.

Vona, Leonard W. 2008. *Fraud Risk Assessment: Building a Fraud Audit Program*. Hoboken: Wiley.

Vona, Leonard W. 2011. *The Fraud Audit: Responding to the Risk of Fraud in Core Business Systems*. Hoboken: John Wiley & Sons.

Wells, Joseph T. 2007. *Fraud Casebook: Lessons from the Bad Side of Business*. Hoboken: John Wiley & Sons.

Wells, Joseph T. 2011. *Corporate Fraud Handbook: Prevention and Detection*. Hoboken: John Wiley & Sons.

Articles:

Bierstaker, James L., Brody, Richard G. and Pacini, Carl 2006. Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, 21, 520-535.

Bonometti, Robert J., Tang, Jun 2006. A dynamic technique for conducting online survey-based research. *Competitiveness Review: An International Business Journal incorporating Journal of Global Competitiveness*, 16, 97-105.

Carley, Kathleen 1993. Coding Choices for Textual Analysis: A Comparison of Content Analysis and Map Analysis. *Sociological Methodology*, 23, 75-126.

Cobanoglu, C., Warde, B., Moreo, P. J. 2001. A Comparison Of Mail, Fax, And Web-Based Survey Methods. *International Journal of Market Research*, 43, 441-452.

Dommeyer, C. J., Moriarty, E. 1999. Comparing two forms of an e-mail survey: embedded vs. attached. *International Journal of Market Research*, 42, 39-50.

Gottschalk, Petter 2010. Theories of financial crime. *Journal of Financial Crime*, 17, 210-222.

Gunter, Barrie, Nicholas, David, Huntington, Paul, Williams, Peter 2002. Online versus offline research: implications for evaluating digital media. *Aslib Proceedings*, 54, 229-239.

Johnson, Gary G. and Rudesill, Charryl L. 2001. An investigation into fraud prevention and detection of small businesses in the United States: responsibilities of auditors, managers, and business owners. *Accounting Forum*, 25 (March), 56-78.

Kaptein, Muel, Avelino, Scott 2005. Measuring corporate integrity: a survey-based approach. *Corporate Governance*, 5, 45-54.

Krambia-Kardis, M. 2002. A Fraud Detection Model: A Must for Auditors. *Journal of Financial Regulation and Compliance*, 10, 266-278.

Lasko, Alan D. 2009. Preventing damaging effects of asset misappropriation. *Debt*^{3}, July/August, 14-15.

McDonald, Heath, Adam, Stewart 2003. A comparison of online and postal data collection methods in marketing research. *Marketing Intelligence & Planning*, 21, 85-95.

Preston, Carolyn C., Colman, Andrew M. 2000. Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences. *Acta Psychologica*, 104, 1-15.

Ranchhod, Ashok, Zhou, Fan 2001. Comparing respondents of e-mail and mail surveys: understanding the implications of technology. *Marketing Intelligence & Planning*, 19, 254-262.

Seidler, Becky 2011. Canada: Expense Report Fraud: Chump Change Or Damaging Dollars? [online] [cited 1.06.2012]. Available: http://www.mondaq.com/canada/x/140426/White+Collar+Crime+Fraud/Expense+Report+Fraud+Chump+Change+Or+Damaging+Dollars

Sheehan, K. B., Hoy, M. G. 1999. Using E-mail To Survey Internet Users In The United States: Methodology And Assessment. *Journal of Computer Mediated Communication*, 4 (March). [online] [cited 15.06.2013]. Available: http://jcmc.indiana.edu/vol4/issue3/sheehan.html

Sheehan, K. B. 2001. E-mail Survey Response Rates: A Review. *Journal of Computer-Mediated Communication*, 6 (January). [online] [cited 15.06.2013]. Available: http://jcmc.indiana.edu/vol6/issue2/sheehan.html

Tysiac, Ken 2012. Small business, big risk. *Journal of Accountancy*, 214.2 (August), 38-43.

Vanasco, Rocco R. 1998. Fraud auditing. *Managerial Auditing Journal*, 13, 4-71.

Wells, Joseph T. 2001. Why employees commit fraud. *Journal of Accountancy*, 191 (February), 89.

Wells, Joseph T. 2001. Enemies within. *Journal of Accountancy*, December, 31-35.

Wells, Joseph T. 2002. Billing Schemes, Part 1: Shell Companies That Don't Deliver. *Journal of Accountancy*, July, 76-79.

Wells, Joseph T. 2002. Billing Schemes, Part 2: Pass-Throughs. *Journal of Accountancy*, August, 72-74.

Wells, Joseph T. 2002. Billing Schemes, Part 3: Pay-and-Return Invoicing. *Journal of Accountancy*, September, 96-98.

Wells, Joseph T. 2002. Billing Schemes, Part 4: Personal Purchases. *Journal of Accountancy*, October, 105-109.

Wells, Joseph T. 2002. Keep Ghosts Off the Payroll. *Journal of Accountancy*, December, 77–82.

Wells, Joseph T. 2003. The Padding That Hurts. *Journal of Accountancy*, February, 67–69.

Wells, Joseph T. 2003. Protect small business. *Journal of Accountancy*, March, 26-32.

Wells, Joseph T. 2004. Small Business, Big Losses. *Journal of Accountancy*, 198 (December), 42-47.

Reports and other sources:

Association of Certified Fraud Examiners, 1996. *Report to the Nations on Occupational Fraud and Abuse*.

Association of Certified Fraud Examiners, 2007. *Fraud Examiners Manual*.

Association of Certified Fraud Examiners, 2011. *Study of Business Security Risks in Russian Companies*. [online] [cited 15.06.2013]. Available: http://acfe-rus.org/

Association of Certified Fraud Examiners, 2012. *Report to the Nations on Occupational Fraud and Abuse*. [online] [cited 15.06.2013]. Available: http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

Committee of Sponsoring Organization of Treadway Commission, 1992. *Internal Control – Integrated Framework*. New York: AICPA.

Committee of Sponsoring Organization of Treadway Commission, 2006. *Internal Control over Financial Reporting - Guidance for Smaller Public Companies*. New York: AICPA.

Committee on Payment and Settlement Systems 2011. *Payment, clearing and settlement systems in the CPSS countries*. Basel: Bank for International Settlements.

Consideration of Fraud in a Financial Statement Audit. Statement on Auditing Standards (SAS) 99: American Institute of Certified Public Accountants (AICPA), 2002.

International Standards for the Professional Practice of Internal Auditing. Standard 1210.A2: The Institute of Internal Auditors (IIA), 2010.

PricewaterhouseCoopers, 2009. *The Global Economic Crime Survey*.

PricewaterhouseCoopers, 2011. *The Global Economic Crime Survey, Russia*. [online] [cited 15.06.2013]. Available: http://www.pwc.ru/en_RU/ru/forensic-services/assets/Economic-survey-2011-Russia-en.pdf

Regulation on Accounting for Fixed Assets. PBU 6/01: Order of the Ministry of Finance of Russia from 30.03.2001 № 26n.

Regulation on Accounting for Inventories. PBU 5/01: Order of the Ministry of Finance of Russia from 09.06.2001 № 44n.

Russian Federal Law № 209-FZ, 24 July 2007. *On developing small and medium scale entrepreneurship in the Russian Federation*. [online] [cited 10.12.2012]. Available: http://www.bu.edu/bucflp/files/2012/01/Federal-Law-No.-209-FZ-of-2007-on-Developing-Small-and-Medium-Scale-Entrepreneurship.pdf.

The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements. International Standard on Auditing (ISA) 240: International Federation of Accountants (IFAC), 2009.

Homepage of The Russian Federal State Statistics Service. [online] [cited 10.12.2012]. Available: http://www.gks.ru/

Homepage of The Russian SME Resource Centre. [online] [cited 10.12.2012]. Available: http://www.rcsme.ru/

Writing Guide on Conducting Content Analysis. [online] [cited 23.05.2013]. Available: http://writing.colostate.edu/guides/page.cfm?pageid=1309

APPENDIX 1: SURVEY EMAIL INVITATION (IN ENGLISH)

Dear managers and accountants of small enterprises,

I am inviting you to participate in the business survey on occupational fraud and methods of its prevention and detection. Data collected during the survey will be used in my thesis project, which is aimed at defining the "best" practices in the fight against illegal activities. Once the work is complete, the respondents will be able to become acquainted with the research results, if desired.

All responses will be kept completely confidential. Your name will not be attached to any results, and all the findings will be presented in a summary format. The questionnaire is user-friendly, and you should be able to complete it within 10 minutes or less.

I kindly ask you to fill in the questionnaire (attached) with regard to your organization and send it to the e-mail ekaterina.milyutina@gmail.com. I would appreciate your response by 14 of June.

Best regards,
Milyutina Ekaterina

APPENDIX 2: SURVEY EMAIL INVITATION (IN RUSSIAN)

Уважаемые менеджеры и бухгалтера малых предприятий,

Приглашаю Вас принять участие в опросе, посвященном теме мошенничества персонала в организациях и методам его обнаружения и предотвращения. Собранные в результате опроса данные будут использованы в моем дипломном проекте, цель которого – выявить “лучшие” методы борьбы с противоправными действиями. По завершению работы, респонденты смогут ознакомиться с результатами исследования, если того желают.

Все ответы останутся строго конфиденциальными. Ваше имя не будет упоминаться в связи с результатами, и все полученные данные будут представлены в составе общих итогов. Анкета поддерживает дружелюбный интерфейс, что позволяет заполнить ее в течение 10 минут или меньше.

Любезно прошу заполнить анкету (прилагается) в отношении Вашей организации и прислать ее на адрес ekaterina.milyutina@gmail.com. Буду признательна, если Вы ответите до 14 июня.

Всего наилучшего,
Милютина Екатерина

APPENDIX 3: THE RESEARCH QUESTIONNAIRE (IN ENGLISH)

Thank you in advance for your voluntary participation. The purpose of this survey is to gather data on the use of fraud prevention and detection measures in organizations and estimation of their effectiveness. It should take approximately 10 minutes to complete. All responses you provide are confidential and will be compiled into general findings. Information specific to you or your organization will not be identified.

Fraud is an illegal act committed by people inside the organization for their own purposes or enrichment, and which results in losses of company's assets (e.g., cash).
Fraud prevention measures include practices attempted to stop irregularities from occurring.
Fraud detection measures include procedures designed to identify anomalies in business.

Respondent profile

Present job title:

☐ Accountant ☐ Manager

☐ Other (please specify_____)

Age:

☐ under 25 years ☐ 25-34 years ☐ 35-44 years ☐ 45-55 years

☐ above 55 years

Highest educational level obtained:

☐ Bachelor's degree ☐ Specialist's degree ☐ Master's degree

☐ Other (please specify_____)

How long have you been in your current position:

☐ under 5 years ☐ 5-9 years ☐ 10-14 years ☐ 15-20 years

☐ above 20 years

Main business of your organization:

☐ Manufacturing ☐ Wholesale and retail trade

☐ Construction ☐ Services

☐ Other (please specify_____)

Number of full-time employees in your organization:

☐ 1-15 persons ☐ 16-50 persons ☐ 51-100 persons

Fraud questions

1. Does your organization have the following defense practices in place? How would you estimate effectiveness of each measure (regardless of its use in your organization)?

Please indicate below what measures are really in place in your business, and how you estimate effectiveness of each measure from the list in preventing fraud from 1 (completely ineffective) to 7 (completely effective).

Alternatives:
1 – Completely ineffective
2 – Mostly ineffective
3 – Somewhat ineffective
4 – Neither effective nor ineffective
5 – Somewhat effective
6 – Mostly effective
7 – Completely effective

Maintaining and regularly updating an approved vendor list (i.e., a list of vendors considered as acceptable to buy from together with files, containing key company information)	yes ☐ no ☐ 1 2 3 4 5 6 7
Verifying entity's legitimacy before adding a new vendor to the approved vendor list *or* before actual purchasing (e.g., obtaining entity's certificate of the state registration, checking the validity of entity's address, etc.)	yes ☐ no ☐ 1 2 3 4 5 6 7
Setting spending limits (e.g., setting the maximum amount for entertainment expenses)	yes ☐ no ☐ 1 2 3 4 5 6 7
Segregation of duties (i.e., different people are responsible for the custodial, approval and recording/reconciling functions)	yes ☐ no ☐ 1 2 3 4 5 6 7

Background and reference checks before hiring (i.e., verifying educational credentials, contacting prior employer, etc.)	yes ☐ no ☐ 1 2 3 4 5 6 7
Restricted access to business records (e.g., the use of login information to enter the system)	yes ☐ no ☐ 1 2 3 4 5 6 7
Use of authorization (i.e., approval provided by authorized person for conducting inquired transactions)	yes ☐ no ☐ 1 2 3 4 5 6 7
Records management policy (i.e., a set of rules that outline requirements for creating, processing and storing documents)	yes ☐ no ☐ 1 2 3 4 5 6 7
Code of conduct (i.e., a set of rules that clarify legal and ethical grounds of conducting business transactions to employees)	yes ☐ no ☐ 1 2 3 4 5 6 7
Educating staff on fraud detection	yes ☐ no ☐ 1 2 3 4 5 6 7
Fraud hotline (i.e., an anonymous and confidential system to receive tips from different sources about potential fraud and other concerns)	yes ☐ no ☐ 1 2 3 4 5 6 7

2. Does your organization have the following audit procedures in place? How would you estimate effectiveness of each measure (regardless of its use in your organization)?

Please indicate below what measures are really in place in your business, and how you estimate effectiveness of each measure from the list in detecting fraud from 1 (completely ineffective) to 7 (completely effective).

Alternatives: 1 – Completely ineffective
2 – Mostly ineffective
3 – Somewhat ineffective
4 – Neither effective nor ineffective
5 – Somewhat effective

6 – Mostly effective
7 – Completely effective

Matching vendor data with employee data (e.g., comparing phone numbers, bank accounts, etc.)	yes ☐ no ☐ 1 2 3 4 5 6 7
Comparing vendor invoices with approved vendor list	yes ☐ no ☐ 1 2 3 4 5 6 7
Comparing the purchase order against the invoice and against the shipping documents	yes ☐ no ☐ 1 2 3 4 5 6 7
Stock-taking of inventory and/or fixed asset items (i.e., comparing the physical quantity of company's assets to the quantity in the books)	yes ☐ no ☐ 1 2 3 4 5 6 7
Monitoring the nature and quantities of goods and services acquired (i.e., judging the reasonableness of types and quantities of purchased merchandise and services)	yes ☐ no ☐ 1 2 3 4 5 6 7
Reconciliation of employees in the payroll database with employees in the human resources database	yes ☐ no ☐ 1 2 3 4 5 6 7
Verifying hours worked and/or the rates of pay (i.e., comparing hours/rates paid with hours/rates presented on employee time sheets/stored in the personnel files)	yes ☐ no ☐ 1 2 3 4 5 6 7
Conducting financial and business analysis (e.g., trend (horizontal) analysis, vertical analysis, analysis of variances between actual and planned (budgeted) amounts, etc.)	yes ☐ no ☐ 1 2 3 4 5 6 7
Sorting documents (i.e., putting documents in a specific order)	yes ☐ no ☐ 1 2 3 4 5 6 7

Detailed review of documentation (i.e., check of data and document validity and completeness)	yes ☐ no ☐ 1 2 3 4 5 6 7
Confirming with customers/vendors the accuracy of payment/billing	yes ☐ no ☐ 1 2 3 4 5 6 7
Comparing expense reports and enclosed supporting documents (i.e., documents that prove the incurred expenses) to the work schedule	yes ☐ no ☐ 1 2 3 4 5 6 7

Thank you!

APPENDIX 4: THE RESEARCH QUESTIONNAIRE (IN RUSSIAN)

Благодарим заранее за Ваше добровольное участие. Цель данного опроса – собрать данные об использовании мероприятий по предотвращению и обнаружению мошенничества внутри организации и оценки их эффективности. Заполнение анкеты занимает приблизительно 10 минут. Все Ваши ответы являются конфиденциальными и будут представлены в составе общих результатов. Информация, касающаяся лично Вас или Вашей организации, раскрытию не подлежит.

Мошенничество - это противоправное действие, совершаемое людьми внутри организации в своих личных целях или в целях своего обогащения, и приводящее к потерям активов компании (напр., денежных средств).
Меры по предотвращению мошенничества включают в себя практики, направленные на предотвращение нарушений.
Меры по обнаружению мошенничества включают в себя процедуры, разработанные для обнаружения аномалий в бизнесе.

Профиль респондента

Настоящая должность:

☐ Бухгалтер ☐ Менеджер

☐ Другое (пожалуйста, укажите_____)

Возраст:

☐ до 25 лет ☐ 25-34 лет ☐ 35-44 лет ☐ 45-55 лет

☐ свыше 55 лет

Высший полученный уровень образования:

☐ Степень бакалавра ☐ Степень специалиста ☐ Степень магистра

☐ Другое (пожалуйста, укажите_____)

Как долго Вы работаете в занимаемой должности:

☐ до 5 лет ☐ 5-9 лет ☐ 10-14 лет ☐ 15-20 лет

☐ свыше 20 лет

Основная деятельность Вашей организации:

☐ Производство ☐ Оптовая и розничная торговля

☐ Строительство ☐ Предоставление услуг

☐ Другое (пожалуйста, укажите_____)

Численность сотрудников, работающих на полную ставку в Вашей организации:

☐ 1-15 чел. ☐ 16-50 чел. ☐ 51-100 чел.

Вопросы о мошенничестве

1. Какие из нижеследующих превентивных практик применяются в Вашей организации? Как бы Вы оценили эффективность каждого мероприятия (независимо от его использования в Вашей организации)?

Пожалуйста, укажите, какие мероприятия действительно используются в Вашем бизнесе, и как Вы оцениваете эффективность каждого мероприятия из списка в предупреждении мошенничества от 1 (полностью неэффективный) до 7 (полностью эффективный).

Варианты:
1 – Полностью неэффективный
2 – По большей части неэффективный
3 – В некоторой степени неэффективный
4 – Ни то, ни другое
5 – В некоторой степени эффективный
6 – По большей части эффективный
7 – Полностью эффективный

Ведение и регулярное обновление утвержденного списка поставщиков (т.е., списка поставщиков, в соответствии с которым разрешено производить закупки, а также ключевой информации о предприятиях)	да ☐ нет ☐ 1 2 3 4 5 6 7
Проверка юридической легитимности предприятия перед добавлением нового поставщика в утвержденный список поставщиков *или* перед фактической закупкой (напр., запрос свидетельства о государственной регистрации предприятия, проверка достоверности юридического адреса предприятия и т.д.)	да ☐ нет ☐ 1 2 3 4 5 6 7

Введение ограничений по расходным операциям (напр., утверждение максимальной суммы представительских расходов)	да ☐ нет ☐ 1 2 3 4 5 6 7
Распределение должностных обязанностей при осуществлении отдельной деловой операции (т.е., разделение функций инициализации операции, авторизации и ведения/согласования счетов)	да ☐ нет ☐ 1 2 3 4 5 6 7
Проверка анкетных данных и рекомендаций кандидатов при приеме на работу (т.е., проверка подлинности аттестатов, установление контакта с предыдущим работодателем и т.д.)	да ☐ нет ☐ 1 2 3 4 5 6 7
Ограниченный доступ к деловым записям предприятия (напр., использование пароля для входа в систему)	да ☐ нет ☐ 1 2 3 4 5 6 7
Авторизация деловых операций (т.е., разрешение, предоставляемое уполномоченным лицом для проведения запрашиваемых операций)	да ☐ нет ☐ 1 2 3 4 5 6 7
Регламент/инструкция по делопроизводству (т.е., набор правил, устанавливающих требования к созданию, организации движения, учету и хранению рабочих документов)	да ☐ нет ☐ 1 2 3 4 5 6 7
Кодекс делового поведения (т.е., свод правил, разъясняющих сотрудникам юридические и нравственные принципы ведения деловых операций)	да ☐ нет ☐ 1 2 3 4 5 6 7
Обучение персонала навыкам распознавания фактов мошенничества	да ☐ нет ☐ 1 2 3 4 5 6 7
Горячая линия по вопросам мошенничества (т.е., анонимная и конфиденциальная система для получения мгновенных сообщений из различных источников о любом потенциальном акте мошенничества и других угрозах)	да ☐ нет ☐ 1 2 3 4 5 6 7

2. Какие из нижеследующих аудиторских процедур применяются в Вашей организации? Как бы Вы оценили эффективность каждого мероприятия (независимо от его использования в Вашей организации)?

Пожалуйста, укажите, какие мероприятия действительно используются в Вашем бизнесе, и как Вы оцениваете эффективность каждого мероприятия из списка в обнаружении мошенничества от 1 (полностью неэффективный) до 7 (полностью эффективный).

Варианты: 1 – Полностью неэффективный

2 – По большей части неэффективный
3 – В некоторой степени неэффективный
4 – Ни то, ни другое
5 – В некоторой степени эффективный
6 – По большей части эффективный
7 – Полностью эффективный

Сопоставление реквизитов поставщиков с данными персонала (напр., сравнение телефонных номеров, номеров банковских счетов и т.д.)	да ☐ нет ☐ 1 2 3 4 5 6 7
Сопоставление данных полученных счет-фактур с данными утвержденного списка поставщиков	да ☐ нет ☐ 1 2 3 4 5 6 7
Сопоставление содержания полученной счет-фактуры с заказом на покупку и товаросопроводительными документами	да ☐ нет ☐ 1 2 3 4 5 6 7
Инвентаризация материально-производственных запасов и/или основных средств (т.е., выявление фактического наличия имущества предприятия и сопоставление с данными бухгалтерского учета)	да ☐ нет ☐ 1 2 3 4 5 6 7
Контроль характера и количества приобретаемых товаров и услуг (т.е., оценка обоснованности типа и количества закупаемых товаров и услуг)	да ☐ нет ☐ 1 2 3 4 5 6 7
Сверка сотрудников, находящихся в базе данных заработной платы, с сотрудниками, находящимися в базе данных персонала	да ☐ нет ☐ 1 2 3 4 5 6 7
Верификация отработанных часов и/или ставок заработной платы сотрудников (т.е., сравнение данных об оплаченных трудовых часах/ставках с данными о трудовых часах/ставках, указанными в табеле учета рабочего времени/хранящимися в личном деле сотрудника)	да ☐ нет ☐ 1 2 3 4 5 6 7
Анализ финансово-хозяйственной деятельности предприятия (напр., проведение трендового (горизонтального) анализа, вертикального анализа, анализа отклонений фактических показателей от плановых (сметных) и др.)	да ☐ нет ☐ 1 2 3 4 5 6 7
Сортировка документов (т.е., упорядочение документов определенным способом)	да ☐ нет ☐ 1 2 3 4 5 6 7

Детальная проверка документации (т.е., проверка данных и документов на предмет достоверности и полноты)	да ☐ нет ☐ 1 2 3 4 5 6 7
Проведение сверок взаимных расчетов с контрагентами (т.е., обращение к контрагентам с целью подтверждения состояния взаимных расчетов на определенную дату)	да ☐ нет ☐ 1 2 3 4 5 6 7
Сопоставление дат авансовых отчетов и приложенных оправдательных документов (т.е., документов, подтверждающих произведенные расходы) с рабочим графиком	да ☐ нет ☐ 1 2 3 4 5 6 7

Спасибо!